

4 Alimentamos tu conocimiento

Revista de Software Libre ATIX 2008

Colaboradores

Equipo Editorial

Dirección y Coordinación General

Esteban Saavedra López (jesaavedra@opentelematics.org)

Diseño y Maquetación

Jenny Saavedra López (jennysaavedra@hotmail.com)
Esteban Saavedra López (jesaavedra@opentelematics.org)

Colaboración

Williams Chorolque Choque (williamsis@gmail.com)

Herramientas

La edición de esta revista fue realizada de forma integra haciendo uso de Software Libre









Palabra quechua,

con un sentimiento profundo

y con gran significado filosófico

El que lo sabe

El que lo intenta

El que lo puede

El que lo logra

El que lo sabe, el que lo intenta, el que lo puede, el que lo logra

Editorial

Desde el momento en que nos concibieron, mantuvimos estrecha relación primero con nuestra madre, quien día a día nos alimento, ya sea proveyéndonos alimentos desde el punto de vista nutritivo, y también nos alimento desde el punto de vista de conocimiento, sirviéndonos como interfaz hacia el mundo exterior.

La actividad de alimentarnos con el tiempo, no ha disminuido, más al contrario ha aumentado, si bien llega una punto en nuestras vidas que nos valemos por nosotros mismos, esto hace que podamos decidir que, como y cuando alimentarnos, pero también tenemos la posibilidad de decidir si o no contribuir con la alimentación de otros.

Son muchas las formas de poder brindar alimento, pero bien dicen nuestros abuelos: "*la mejor herencia, es la educación que recibimos*", y por ende el decidir alimentarnos día tras día de mayores y mejores conocimientos, hace que crezcamos como personas.

Alimentamos tu conocimiento, un título que encierra el pequeño, pero gran aporte que hemos venido realizando en nuestros primeros números en la revista, números que han contenido artículos, a lo mejor sencillos pero que han contribuido a alimentar el conocimiento de los recién empiezan a introducirse en este maravilloso mundo del software libre, y también una forma de compartir el conocimiento que otros han adquirido alimentando el suyo propio.

En éste cuarto número ponderamos aspectos como la entrevista a **Julian Fagotti** coordinador de la **Conferencia Latino Americana de Software Libre LATINOWARE**, a quién ofrecemos nuestra gratitud por concedernos una entrevista; un segundo aspecto va referido a la participación de algunos investigadores que recién empiezan y son entusiastas del Software Libre.

Alimenta tu conocimiento hoy y siempre.

Bienvenidos a nuestro cuarto número

Esteban Saavedra López
Director y Coordinador General

Contenido

Liberado el 17 de septiembre de 2008



Frontends para nuestros Shell Scripts

Los diálogos son utilidades que sirven para crear interfaces a shell scripts, u otros lenguajes como Perl y Python. Muchos de éstas utilidades no son gráficas (utiliza curses) así es que puede funcionar bien en cualquier consola. Hay versiones gráficas llamadas Xdialog con variantes para Gnome y KDE.

Introducción

Para las personas que estamos aprendiendo a programar shell scripts y que deseamos que nuestros programas tengan una interfaz que nos ayude a manejarla, es importante contar con utilidades como Dialog o de forma genérica con XDialog, que en su mayoría tienen los paquetes disponibles para cualquier distribución.

Estas utilidades inicialmente sólo estaban disponibles para funcionar dentro de un entorno en modo texto, pero actualmente se han actualizado de tal forma que nos permiten trabajar en modo texto, modo gráfico y poseen algunas especificaciones para algunos lenguajes específicos como es el caso de **Udpm (User Dialog Perl Modulates)** y **pythondialog**

Diálogos de forma general

Simplemente son utilidades que nos permiten crear interfaces (texto o gráfica) para nuestros shell scripts o para algún lenguaje especifico.

Porqué usar Diálogos?

Porque dentro de nuestros shell scripts, podremos aprovechar las ventajas que se encuentran dentro de estas utilidades; en ningún caso debemos programar o desarrollar estos diálogos, por que ya están listos para invocarlos y hacer uso de ellos

Características de los Diálogos

- ✔ Fáciles e intuitivos de aprender y utilizar.
- ✔ Nos permiten hacer uso de los diálogos más genéricos y más frecuentemente necesarios para desarrollar cualquier shell script
- ✔ Disponibles tanto para trabajar tanto en modo texto como en modo gráfico

Pasos para crear interfaces para nuestros Shell Scripts

- ✔ Instalar la utilidad, que está presente en todas las distribuciones actuales.
- ✔ Revisar la documentación de la utilidad correspondiente y ver la forma de uso de cada diálogo.
- ✔ Incluir el diálogo en nuestros shell scripts.
- ✔

Diálogos existentes

Entre las utilidades para realizar diálogos se encuentran:

- ✔ Dialog
- ✔ Whiptail
- ✔ gdialog
- ✔ Xdialog
- ✔ Zenity
- ✔ Kdialog
- ✔ Udpm (User Dialog Perl Modulates)
- ✔ pythondialog

Qué se pueden hacer con los diálogos

Habilitar interfaces que permitan hacer uso de recursos como:

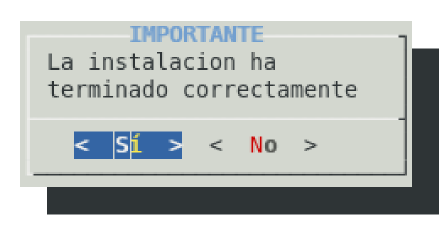
- ✔ Calendario y Hora
- ✔ Cajas de mensajes (messagebox)
    - ✔ Error
    - ✔ Información
    - ✔ Preguntas
    - ✔ Alerta
- ✔ Cajas de entrada de texto (inputbox, editbox)
- ✔ Listas de opciones(listbox, combobox)
- ✔ Listas de opciones (radiobuttons, checkbox)
- ✔ Selección de archivos o directorios(selectfile)
- ✔ Vistas jerárquicas(treeview)
- ✔ Progreso de operaciones
- ✔ Mensajes en el área de notificación
- ✔ etc.

Algunas posibilidades de estas utilidades

En internet podemos encontrar una gran cantidad de ejemplos de estas utilidades, pero para los que recién empiezan como yo, es bueno verlos en acción, así que a continuación realizaremos una revisión de algunas posibilidades de estas utilidades.

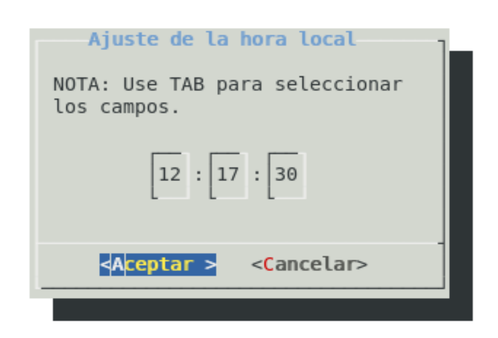
Dialog

Cajas de diálogo



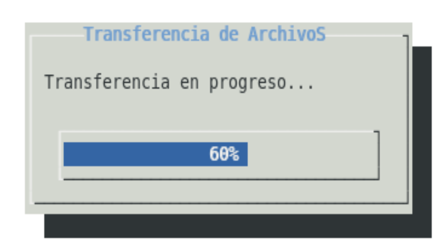

```
dialog  \
   --title 'IMPORTANTE' \
   --yesno 'La instalacion ha terminado
correctamente'  \
   0 0
```

Asignación de hora



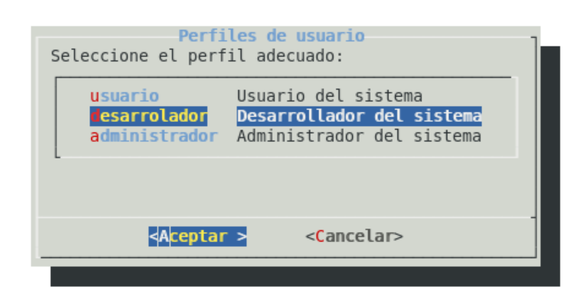

```
dialog  \
   --title 'Ajuste de la hora local' \
   --timebox '\nNOTA: Use TAB para seleccionar
los campos.'  \
   0 0  \
   12 17 30
```

Progreso de operaciones



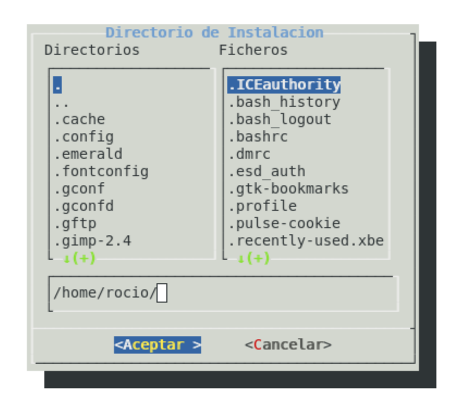

```
dialog  \
   --title 'Transferencia de ArchivoS'  \
   --gauge '\nTransferencia en progreso...'  \
   8 40 60
```

Menú de opciones



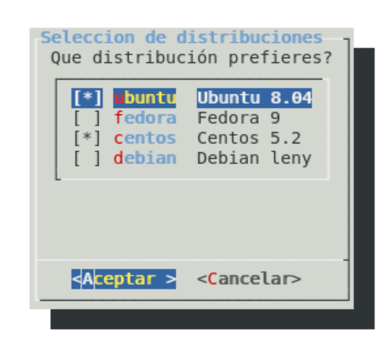

```
dialog  \
   --title 'Perfiles de usuario'  \
   --menu 'Seleccione el perfil adecuado:'  \
   0 0 0 \
   usuario 'Usuario del sistema' \
   desarrolador 'Desarrollador del sistema'  \
   administrador 'Administrador del sistema'
```

Diálogo estándar de selección de directorio




```
dialog \
   --title 'Directorio de Instalacion'  \
   --fselect /home/rocio/ \
   10 45
```

Lista de opciones




```
dialog  \
 --title 'Seleccion de distribuciones' \
 --checklist 'Que distribución prefieres?'  \
   0 0 0  ubuntu 'Ubuntu 8.04' on  \
   fedora 'Fedora 9' off  \
   centos 'Centos 5.2' on  \
   debian 'Debian leny' off
```

XDialog

Lista de opciones




```
Xdialog --title "Distribuciones" \
        --combobox "Selección de una
distribución" \
        0 0 "Ubuntu 1" "Fedora 2" "CentOS 3"
"Debian 4" \
        "Mandriva 5"
```

Rango de valores




```
Xdialog --title "Porcentaje de avance" \
        --rangebox "Valor del porcentaje
avanzado" 0 0 1 100 60
```

Escala de valores




```
Xdialog --title "Valoracion del evento" \
        --spinbox "¿Qué nota le das al
evento?" 0 0 1 10 9 "Nota"
```

Diálogo estándar de selección de color




```
Xdialog --title "Seleccion de Color" \
        --colorsel "Color de la paleta" 18 55
50 60 70
```

Vistas jerárquicas




```
Xdialog --title "Arbol de proyectos"
--treeview \
            "Clasificacion" 0 0 0 \
            "General" "Generales" "off" 1 \
            "Internet" "Internet" "off" 2 \
              "Firefox" "Firefox" "off" 3 \
              "Pidgin" "Pidgin " "off" 3 \
            "Oficina" "Ofimaticas" "off" 1 \
              "OpenOffice" "OpenOffice" "off"
2 \
              "Kile" "Kile" "off" 2 \
```

Construcción de listas




```
Xdialog --title "Distribuciones disponibles" \
        --buildlist "Seleccione  las
distribuciones" \
        0 0 0 "ubuntu" "Ubuntu" "on" "fedora"
"Fedora" "off" \
        "debian" "Debian" "on" "centos"
"CentOS" "off"
```

KDialog

Cajas de diálogo



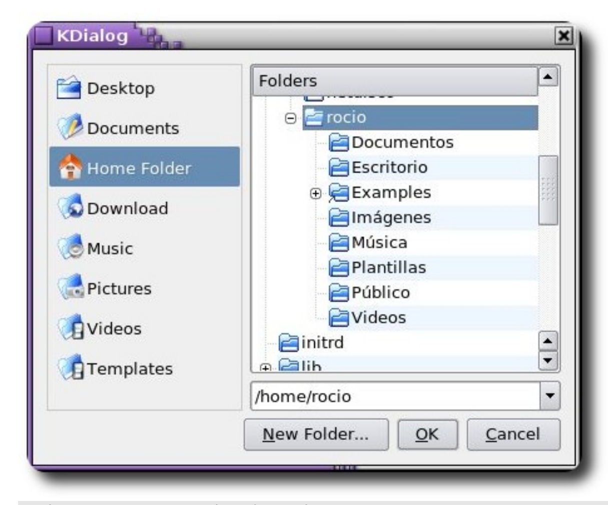

```
kdialog --title "Instalaciones" \
        --yesnocancel "Desea realizar la
instalación"
```

Entradas de texto con valores definidos




```
kdialog --title "Entrada de datos" \
        --inputbox "Nombre de usuario" \
        "Usuario por defecto"
```

Diálogo estándar de selección de directorio




```
kdialog --getexistingdirectory .
```

Entrada de contraseñas



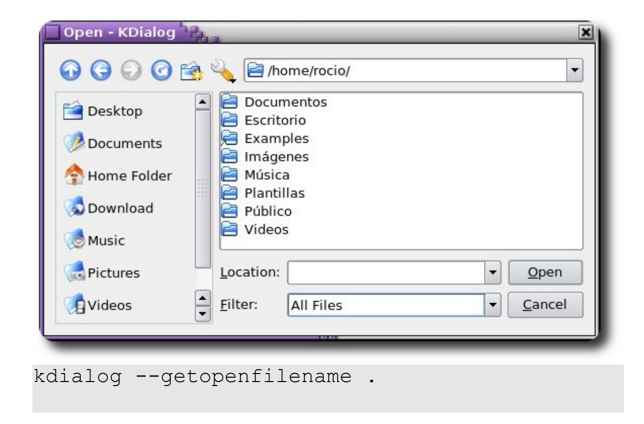

```
kdialog --title "Autenticacion" \
        --password "ingrese la palabra clave:"
```

Menú de opciones




```
kdialog --radiolist "Seleccione el idioma:" \
        1 "Ingles" off  2  "Castellano" on 3
"Frances" off
```

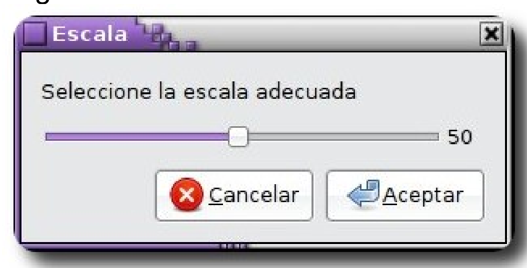
Diálogo estándar de selección de directorio




```
kdialog --getopenfilename .
```

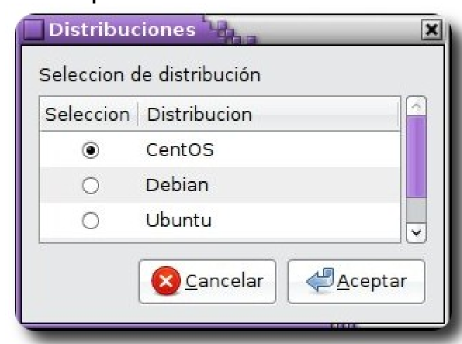
Zenity

Rango de valores




```
zenity --scale --title "Escala"\
       --text "Seleccione la escala
adecuada" \
       --min-value=2 --max-value=100
--value=50 --step 2
```

Listas de opciones



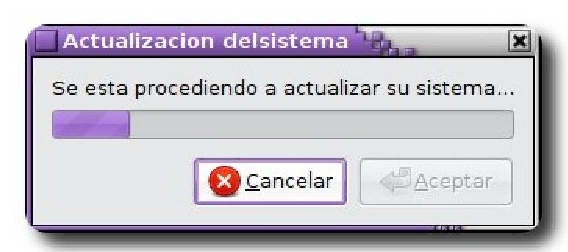

```
zenity  --list  --title "Distribuciones"\
        --text "Seleccion de distribución" \
        --radiolist  --column "Seleccion"
--column "Distribucion" TRUE \
        "CentOS" FALSE "Debian" FALSE "Ubuntu"
FALSE "Ninguna"
```

Lista de opciones



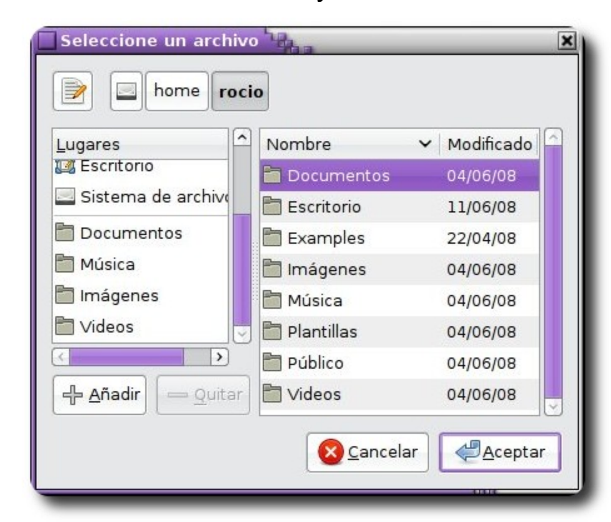

```
zenity  --title "Aplicaciones disponibles"
--list  \
--text "Seleccione una aplicacion" \
--checklist  --column "Check" --column
"Opcion" \
TRUE "OpenOffice" TRUE "Firefox" FALSE
"Gimp" \
FALSE "Inkscape" --separator=":"
```

Progreso de operaciones




```
zenity --progress --title="Actualizacion
delsistema" \
       --text="Se esta procediendo a
actualizar su sistema..." \
       --percentage=17
```

Selección de archivos y directorios




```
zenity --file-selection --title="Seleccione un
archivo"
```

Dialogo de notificación




```
zenity --notification\
         --window-icon="info" \
         --text="!Hay actualizaciones que son
necesarias para su sistema!"
```

Interfaces para lenguajes específicos

Cuando existan oportunidades de desarrollar programas en lenguajes como **Perl** y **Python**, podemos hacer uso de utilidades como **Udpm (User Dialog Perl Modulates)** y **pythondialog**, que nos permiten habilitar interfaces como las vistas en éste artículo, pero orientadas directamente a estos lenguajes.

Conclusiones

El uso de utilidades como **Dialog, XDialog, KDialog, Zenity**, facilitan enormemente el desarrollo de shell scripts con una interfaz adecuada e intuitiva para el usuario final.

Referencias

[1] http://linux.die.net/man/1/dialog

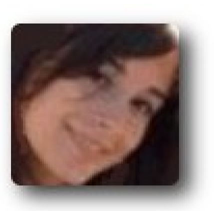
[2] http://xdialog.dyns.net/

[3] http://xdialog.free.fr/doc/box.html

[4] http://live.gnome.org/Zenity

[5] http://techbase.kde.org/Development/Tutorials/Shell_Scripting_with_KDE_Dialogs

Autor



Rocio Figueroa
Estudiante de Ingeniería en Telecomunicaciones
rocios.figueroa@gmail.com

Introducción a Django (2da parte)

Django es un framework para el desarrollo de aplicaciones Web desarrollado en Python originalmente por Adrian Holovaty, Simon Wilson, Jacob Kaplan-Moss y Wilson Miner para World-Online el 2003 . Desde 2005 es software de código abierto (con una licencia BSD) y en septiembre de 2008 alcanzará la tan ansiada versión 1.0.



Introducción

En esta entrega vamos a integrar una aplicación adicional, contact_form, para tener un formulario de contacto en nuestro sitio y vamos a aprender más sobre las plantillas en Django.

Instalando contact_form.

contact_form, **`http://code.google.com/p/django-contact-form/`**, es una aplicación que nos proporciona un formulario de contacto genérico que recibirá un mensaje en nuestro sitio Web y lo hará llegar a través de correo electrónico a los administradores del sitio.

Partimos de la versión de desarrollo de **`contact_form`**, directamente desde el repositorio Subversion del proyecto [a]:

```
$ cd ~/Development
$ svn checkout http://django-contact-
form.googlecode.com/svn/trunk/ \
    django-contact-form-read-only
```

Luego podemos instalar **`contact_form`** ejecutando **`setup.py`** directamente o haciendo un enlace directo al código desde nuestro directorio **`site-packages`**:

```
$ cd ~/lib/python2.5/site-packages
$ ln -s ~/Development/django-contact-
form/contact_form
$ export PYTHONPATH=~/lib/python2.5/site-
packages:~/Projects
```

En nuestro poyecto (atix) es necesario activar la aplicación **`contact_form`**, añadiéndola a nuestra lista de aplicaciones instaladas en **`settings.py`**:

```
INSTALLED_APPS = (
    ...
    'contact_form',
)
```

Además es necesario configurar adecuadamente **`MANAGERS`**, quienes serán los que reciban el mensaje, y **`DEFAULT_FROM_EMAIL`** que será el remitente del mensaje.

Es posible configurar Django para que envíe los mensajes a través de una cuenta de Gmail por ejemplo, sólo es necesario añadir lo siguiente a **`settings.py`**:

```
EMAIL_HOST = 'smtp.gmail.com'
EMAIL_HOST_USER = 'usuario@gmail.com'
EMAIL_HOST_PASSWORD = 'tu_contraseña'
EMAIL_PORT = 587
EMAIL_USE_TLS = True
```

Como la aplicación **`contact_form`** no define ningún modelo, no es necesario sincronizar la base de datos, lo único que falta es crear las plantillas; pero antes algo más sobre las plantillas.

Plantillas en Django.

El lenguaje de las plantillas en Django es similar al de Smarty y Cheetah Templates, y es básicamente un archivo de texto que contiene variables, filtros y etiquetas. Las variables son sustituidas por sus valores, modificados por los filtros y las etiquetas controlan la lógica.

Variables y fitros.

Las variables son objetos que las plantillas reciben de las vistas, son sustituídas por su valor y están marcadas dentro de las plantilla con **`{{ variable }}`**.

Estas variables pueden ser listas, diccionarios o simplemente objetos que vienen directamente de la base de datos. En cada uno de los objetos se puede hacer referencia a atributos del mismo, que pueden ser atributos de la instancia, elementos de una lista, tupla o diccionario e incluso métodos del mismo.

En la plantilla para la página estática **`flatpages/default.html`** por ejemplo hacíamos referencia a atributos title y content del objeto flatpage mediante un punto ".". De la misma manera podríamos hacer referencia a otros atributos de la variable flatpage como ser **`registration_required`** y **`enable_comments`**, que definen si el usuario debe estar registrado (identificado) para poder ver la página y si es posible dejar comentarios en la página respectivamente.

Los filtros se pueden aplicar directamente a las variables para cambiar su contenido o formatearlo. Se aplican mediante la barra vertical (pipe) "|", inmediatamente después de la variable. **`{{ variable|filtro }}`**.

Por ejemplo en la plantilla **`flatpages/default.html`** usábamos el filtro safe para marcar el contenido de la variable como seguro. La lista de filtros es larga y está disponible en la documentación oficial de las plantillas: **http://docs.djangoproject.com/en/1.0/topics/templates/.**

Etiquetas.

Las etiquetas controlan la lógica de la plantilla, están marcadas en las plantillas con **`{% etiqueta %}`**, algunas crean texto adicional, otras controlan el flujo dentro la plantilla, definiendo bucles y condicionales, y otras cargan contenido (externo) a variables. Algunas requieren además de una etiqueta de apertura y cierre:

```
{% etiqueta %}
  ...
{% endetiqueta %}.
```

La lista completa de etiquetas disponibles en la documentación oficial: **http://docs.djangoproject.com/en/1.0/ref/templates/builtins/**

De éstas vamos a usar inicialmente dos: extends y block.

- ✔ **{% extends "..." %}** Señala que la plantilla extiende (se deriva) de otra plantilla. La etiqueta puede ser usada de dos maneras:
- ✔ **{% extends "base.html" %}** usa el valor literal "base.html" como el nombre de la plantilla que se extiende.
- ✔ **{% extends variable %}** usa el valor de la variable que puede representar al nombre de la plantilla (archivo) o a un objeto del tipo Template.
- ✔ **{% block ... %}...{% endblock %}** define un bloque que puede ser extendido por otra plantilla o la manera en que un bloque será reemplazado al ser extendido.

Podemos definir por ejemplo un bloque con el título de nuestro sitio en una plantilla **`base.html`** con:

```
{% block title %}ATIX{% endblock %}
```

Y luego añadir el título de las páginas estáticas en su respectiva plantilla, **`flatpages/default.html:`**

```
{% block title %}{{ flatpage.content }}
| {{ block.super }}{% endblock %}
```

La variable **`{{ block.super }}`** será reemplazada por el contenido del bloque en la plantilla base que estamos extendiendo.

Con todo esto en mente vamos a crear una plantilla base para nuestro sitio y la extenderemos de acuerdo a las necesidades de nuestras páginas estáticas y de nuestro formulario de contacto.

Plantilla base.

La plantilla base es aquella que define la estructura global de nuestro sitio y de la que se derivarán todas las demás, evitando así el repetir todo aquello que tiene un común todo el sitio en cada una de las plantillas que use nuestro sitio.

En este caso simplemente definimos dos bloques title y content.

templates/base.html

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML
4.01//EN"
"http://www.w3.org/TR/html4/strict.dtd">
<html>
<head>
    <title>{% block title %}atix{%
endblock %}</title>
</head>

<body>
    <h1>ATIX</h1>

    <hr>

    {% block content %}{% endblock %}

    <hr>
</body>

</html>
```

Plantilla para las páginas estáticas (flatpages)

La plantilla por defecto para las páginas estáticas simplemente se deriva de la plantilla base y adiciona al título de la página el título de la misma. El contenido mismo de la página es reemplazado por el contenido de la página estática.

templates/flatpages/default.html

```
{% extends "base.html" %}

{% block title %}{{ flatpage.title }} |
{{ block.super }}{% endblock %}

{% block content %}
    {{ flatpage.content|safe }}
{% endblock %}
```

Plantillas para el formulario de contacto (contact_form).

El formulario de contacto utiliza cuatro plantillas, dos para generar en formulario de contacto mismo y la notificación de que el mensaje ha sido enviado y otras dos para generar el asunto y el mensaje mismo que será enviado por correo electrónico.

La única variable disponible en la plantilla del formulario es form, que contiene el formulario mismo con los atributos name, email y body.

Esta plantilla es rudimentaria pero aún así contiene validación automática. Más adelante en esta serie estaremos ampliando y mejorando esta plantilla.

templates/contact_form/contact_form.html

```
{% extends "base.html" %}

{% block title %}Contacto{% endblock %}

{% block content %}
<h2>Contacto</h2>

<p>
<form action="." method="POST">
    <table>
        <tr>
            {{ form.as_table }}
        </tr>
    </table>

    <input type="submit" value="enviar el
mensaje">
</form>
{% endblock %}
```

templates/contact_form/contact_form_sent.html

```
{% extends "base.html" %}

{% block title %}Mensaje enviado{% endblock %}

{% block content %}
<h2>Gracias</h2>

<p>
Tu mensaje ha sido enviado, Gracias.
</p>
{% endblock %}
```

El mensaje de correo electrónico será generado usando dos plantillas, la primera se encarga del asunto que tendrá el mensaje, la segunda define el contenido del mensaje.

templates/contact_form/contact_form_subject.txt

```
{{ site.name }}: Contacto
templates/contact_form/contact_form.txt
Mensaje enviado por {{ name }}
{{ email }}
{{ body }}
```

En la próxima entrega perfeccionaremos nuestras plantillas usando Blueprint, un framework para hojas de estilo (CSS) y daremos el primer paso hacia la creación de nuestra primera aplicación aprendiendo sobre modelos en Django.

Notas:

[a] La última versión estable de contact_form disponible al momento de escribir este artículo (0.3) no es compatible con la versión 1.0 beta de Django en la que se basa esta serie de artículos.

Referencias

[1] http://www.djangoproject.com/

Autor



Ernesto Rico Schmidt

Usuario de Linux y Software Libre desde 1994
e.rico.schmidt@gmail.com

Conociendo PostgreSQL

PostgreSQL es un servidor de base de datos relacional orientada a objetos de software libre, publicado bajo la licencia BSD.



Introducción

En esta ocasión hablaremos un poco sobre PostgreSQL un Sistema de gestión de Bases de Datos libre, bajo una licencia BSD.

Primero que nada decir que no soy un experto en el tema de manejar PostgreSQL de hecho lo vengo usando hace aproximadamente un año pero honestamente me gusto aprender y trabajar con PostgreSQL por eso me anime a escribir un poco de lo que aprendí, lo que veremos en este artículo es como instalar PostgreSQL desde fuentes y como realizar una configuración básica para empezar a trabajar con algun frontend.

Ahora el porque desde fuentes? Si bien pueden encontrar en los repositorios de su distribución todo lo necesario para instalar PostgreSQL pienso que nunca esta demás recordar y sufrir un poco (en realidad aprender) con la instalación desde fuentes ya que es mas personalizada y tenemos el control total además que tenemos una flexibilidad total en cuanto a que es lo que queremos instalar aunque el inconveniente de las actualizaciones puede hacernos pensar un poco sobre si es lo más adecuado pero vamos a lo nuestro.

Comenzando con PostgreSQL

Instalación de PostgreSQL

Primero crearemos un usuario llamado postgres como root tecleamos lo siguiente

```
adduser --home /home/postgres postgres
```

introducimos los datos que nos solicita como ser una contraseña para nuestra cuenta, un nombre de usuario, pueden dejar algunos campos vacíos presionando ENTER, finalmente presionamos la tecla “y” para indicar que estamos de acuerdo con los cambios realizados.

Una vez creada esta cuenta es hora de ingresar a ella con

```
su – postgres
```

ahora configuraremos algunas variables de entorno, por lo tanto editaremos el archivos **.bashrc**

```
vim .bashrc
```

o algún editor de su preferencia al final de dicho archivo podemos añadir lo siguiente:

```
export PGDATA=$HOME/data
export PGLOG=$PGDATA/server.log
export PGSRC=$HOME/src
export PGHOME=$HOME/pgsql
export PGBIN=$HOME/pgsql/bin
```

Veamos cual es el propósito de cada uno de las variables de entorno:

- ✔ **PGDATA** es la ubicación del cluster
- ✔ **PGLOG** el fichero que registrara todo el movimiento existente en el servidor

- **PGSRC** lugar donde se ubica el código fuente de postgreSQL.
- **PGHOME** lugar donde se instalará postgreSQL
- **PGBIN** lugar donde están todos los programas de postgreSQL

tendremos que recargar nuestras archivo de configuración por lo tanto tecleen lo siguiente : **source .bashrc ,** si ejecutamos **echo $PGDATA,** podremos ver el contenido de esta variable de entorno que tendría que ser el valor que le colocamos anteriormente, si todo esta bien continuemos sino revisen nuevamente el archivo anterior.

Hora de descargar el código fuente

Lo primero es descargar el código fuente desde la pagina de PostgreSQL **www.postgresql.org** en la sección download podemos conseguir la ultima versión que en el momento de escribir este articulo era la versión 8.3.3 la pueden descargar comprimido en **tar.gz** o **tar.bz2** o en .bin en nuestro caso descargamos el archivo **postgresql-8.3.3.tar.bz2** lo copiamos al directorio raíz de nuestro usuario postgres, y lo descomprimimos con

```
tar jxvf postgresql-8.3.3.tar.bz2
```

si lo descargamos en formato **.tar.gz** usaremos

```
tar xzvf  postgresql-8.3.3.tar.gz
```

ahora a cambiarle de nombre con

```
mv  postgresql-8.3.3 src
```

para que tenga concordancia con las variables de entorno que definimos anteriormente, hora de la compilación por lo cual es necesario tener instalado el compilador de C que es **gcc** si no lo tienen instalado para instalarlo lo mas simple es instalar el paquete **build-essential** que instalara todo lo necesario, también es necesario tener instalado otras librerías como ser: **gettext , readline , zlib** , etc

podemos ver las distintas opciones de compilación ingresando la directorio donde se encuentran las fuentes y ejecutando:

```
cd $PGSRC
./configure --help
```

Hora de instalar

Una vez visto las opciones de instalación instalaremos de la siguiente manera (si desean una explicación mas detallada de cada una de las opciones ejecuten el anterior comando)

```
$PGSRC/configure --prefix=/home/postgres/
pgsql --with-pgport=5432  --with-python
```

donde:

- **--prefix:** Es la ruta donde se instalará PostgreSQL.
- **--with-pgport**: Es el puerto que escuchará el Servidor aunque este puerto ya es el por defecto.
- **--with-python**: Módulo para PL/Python

si todo a ido bien ejecutamos dentro del directorio **$PGSRC** si tenemos algún error con python lo podemos quitar o instalar el paquete **python-dev** ahora ejecuten **make** y luego cambiamos a root e ingresamos al directorio **/home/postgres/src** y ejecutamos **make install .** Una vez concluido la instalación volvamos a nuestra cuenta de postgres y configuremos algunas variables de entorno adicionales así que a abrir el archivo **.bashrc** y añadimos lo siguientes

```
export PATH=$PGBIN:$PATH
export MANPATH=$PGHOME/man:$MANPATH
export LD_LIBRARY_PATH=$PGHOME/lib:
$LD_LIBRARY_PATH
export PGHOST=localhost
export PGPORT=5432
```

Y que son estas variables de entorno:

- **PATH** Incluimos PGBIN que es donde se encuentran todos los ejecutables de PostgreSQL al path de nuestro usuario postgres.
- **MANPATH** Incluimos el directorio de los manuales.

- **LD_LIBRARY_PATH** Incluimos el directorio de librerías.
- **PG_HOST** host del Servidor de PostgreSQL
- **PGPORT** Puerto que escuchará el servidor.

nuevamente recargamos este archivo con **`source .bashrc`**, una vez concluido con la instalación debemos de iniciar nuestro cluster para lo cual usamos el siguiente comando : **`initdb --pgdata=$PGDATA --encoding=utf8 –locale=es_ES`** , utf8 lo pueden cambiar por LATIN1 si tienen algunos problemas con caracteres especiales y finalmente iniciamos el postmaster indicando donde se encuentra el cluster y el archivo de seguimiento al servidor.

```
pg_ctl -D $PGDATA -l $PGLOG start
```

una vez hecho esto podemos conectarnos a nuestro servidor ejecutando la sentencia **`psql`** , desde donde podemos administrar nuevo Sistema Gestión Base de Datos para salir de psql solo escriban **`\q`** y listo.

```
postgres@TuX: ~
Archivo Editar Ver Terminal Solapas Ayuda
postgres@TuX:~$ psql
Welcome to psql 8.3.3, the PostgreSQL interactive terminal.

Type:  \copyright for distribution terms
       \h for help with SQL commands
       \? for help with psql commands
       \g or terminate with semicolon to execute query
       \q to quit

postgres=#
```

Creando una Base de Datos

Bueno después de tanto trabajo para instalar veamos algunos comando de psql primero tenemos a:

- **\?** que es un comando que nos permite ver todos los posibles comandos de psql.
- **\l** Nos permite listar todas las Bases de Datos que tengamos creadas (ojo que es ele de list).
- **\c** seguido de un nombre de base de datos nos permite conectarnos a dicha base de datos.
- **\dt** Con este comando podemos ver todas las tablas que contiene la Base de datos a la cual estamos conectados
- **\d** Seguido de un nombre de una tabla nos permite conocer la tabla, índice, vista o secuencia que le pasemos como parámetro.
- **\q** Salir de psql

Pero mejor lo veamos con un pequeño ejemplo:

Creando una Nueva Base de Datos

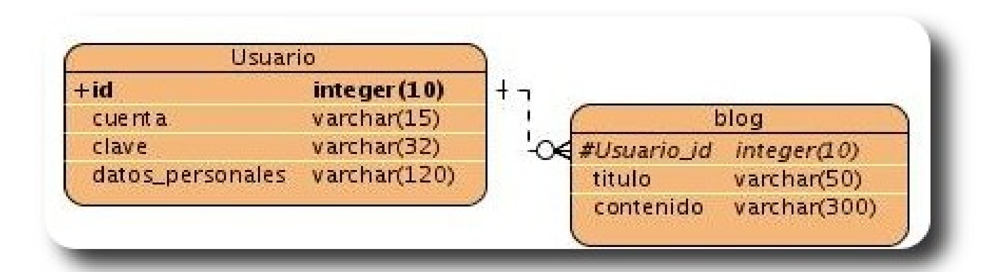
Dentro de psql ejecutemos lo siguiente **`CREATE DATABASE atix`**; con lo cual tenemos creado nuestra base de datos si ejecutamos el comando **`\l`** podremos ver nuestra base de datos. Una alternativa es crear la Base de Datos desde la cuenta de postgres osea desde el shell para ello tenemos que ejecutar la sentencia **`createdb atix`**.

Conectándose a nuestra Base de Datos

Una vez creado nuestra Base de Datos tenemos que conectarnos a ella para lo cual ejecutamos **`\c atix`** en el prompt nos informará que estamos conectados a la base de datos atix.

Creando Tablas

Ahora plasmaremos el siguiente modelo en nuestra Base de Datos:



Primero creamos nuestro tabla usuario pero antes de eso es necesario ver que la clave principal es de tipo entero y se auto incrementará en postgreSQL existe un tipo de dato para este caso que es el SERIAL que no es mas que una secuencia pero en este ejemplo crearemos dicha secuencia a mano por lo tanto el código para realizar esto seria:

```
CREATE SEQUENCE usuario_seq;
CREATE TABLE usuario(
id INTEGER DEFAULT NEXTVAL('usuario_seq'),
cuenta VARCHAR(15),
clave VARCHAR(32),
datos_personales VARCHAR(120),
CONSTRAINT usuario_pk PRIMARY KEY (id),
CONSTRAINT check_cuenta CHECK(length(trim(cuenta))>0),
CONSTRAINT check_clave  CHECK(length(trim(clave))>0),
CONSTRAINT check_datos_personales CHECK(length(trim(datos_personales))>0)
);
```

Veamos que hicimos en todo esto, además de crear la tabla le dimos algunas restricciones como que cuenta, clave y datos personales no pueden estar vacíos. Ahora crearemos la segunda Tabla que esta relacionada con la tabla usuario.

```
CREATE TABLE blog(
usuario_id INTEGER,
titulo VARCHAR(50),
contenido VARCHAR(300),
CONSTRAINT blog_fk FOREIGN KEY(usuario_id) REFERENCES usuario(id),
CONSTRAINT check_titulo CHECK(length(trim(titulo))>0),
CONSTRAINT check_contenido CHECK(length(trim(contenido))>0)
);
```

listo con esto ya tendríamos nuestra base de datos lista si queremos ver como estan definidos estas tablas lo único que tenemos que hacer es \d usuario o \d blog provemos un poco nuestra base de datos y insertemos 2 registros e inmediatamente veamos lo que hemos insertado para lo cual ejecutamos lo siguiente:

```
INSERT INTO usuario(cuenta, clave, datos_personales)
VALUES('WILLIAMS', MD5('WILLIAMS'), 'WILLIAMS'),
('ISRAEL', MD5('ISRAEL'), 'ISRAEL') RETURNING *;
```

con lo cual obtenemos el siguiente resultado:

```
                              Tabla «public.usuario»
    Columna      |          Tipo          |                  Modificadores
-----------------+------------------------+---------------------------------------------------
 id              | integer                | not null default nextval('usuario_seq'::regclass)
 cuenta          | character varying(15)  |
 clave           | character varying(32)  |
 datos_personales | character varying(120) |
Índices:
    «usuario_pk» PRIMARY KEY, btree (id)
Restricciones CHECK:
    «check_clave» CHECK (length(btrim(clave::text)) > 0)
    «check_cuenta» CHECK (length(btrim(cuenta::text)) > 0)
    «check_datos_personales» CHECK (length(btrim(datos_personales::text)) > 0)

atix=# \d blog
                 Tabla «public.blog»
  Columna   |          Tipo          | Modificadores
------------+------------------------+---------------
 usuario_id | integer                |
 titulo     | character varying(50)  |
 contenido  | character varying(300) |
Restricciones CHECK:
    «check_contenido» CHECK (length(btrim(contenido::text)) > 0)
    «check_titulo» CHECK (length(btrim(titulo::text)) > 0)
Restricciones de llave foránea:
    «blog_fk» FOREIGN KEY (usuario_id) REFERENCES usuario(id)

atix=# INSERT INTO usuario(cuenta, clave, datos_personales) VALUES('WILLIAMS', MD5('WILLIAMS'), 'WILLIAMS'),('I
SRAEL', MD5('ISRAEL'), 'ISRAEL') RETURNING *;
 id |  cuenta  |              clave               | datos_personales
----+----------+----------------------------------+------------------
  1 | WILLIAMS | 6ef709d1ac2133083da9be010d81d1d2 | WILLIAMS
  2 | ISRAEL   | 3c08b05a853446689e038b1d3471cfa5 | ISRAEL
(2 filas)

INSERT 0 2
atix=#
mplayer | Consola
williams@TuX: ~ - KDE Terminal Emulator
```

Para terminar en psql podemos hacer absolutamente todo así que nunca esta demás aprender a usar esta herramienta.

Finalmente para terminar nuestra sesión escriban **`\q`** con eso terminaríamos ese pequeño paseo por psql.

para detener el Servidor ejecutamos **`pg_ctl stop`**

No olviden volver a arrancar el servidor cada vez que inician su ordenador y quieran trabajar con postgreSQL. (siempre que no lo tengan configurado para que se inicie al arrancar el ordenador)

Herramientas de Administración de PostgreSQL

Si bien psql constituye una gran herramienta con la que podemos realizar toda la administración de nuestro Servidor en algunas ocasiones buscamos algunas herramientas que nos faciliten mucho más el trabajo y es por eso que aquí les voy a mencionar alguna de ellas.

PhpPgAdmin

Esta es una gran herramienta ya que nos permite tener el control total de nuestro servidor desde un entorno web, aquí les describiré como pueden realizar la instalación y configuración a partir desde fuentes (También lo pueden encontrar en los repositorios de su distribución), así que manos a la obra.

Instalación de PhpPgAdmin

Si bien con psql podemos tener el control total, a veces por queremos un entorno mas amigable o mas fácil de manejar y podemos probar instalando pgadmin3 que es muy bueno también tenemos phppgadmin que es muy bueno y en esta ocasión instalaremos este para lo cual seguiremos los siguientes pasos.

Descargamos el archivo **phpPgAdmin-4.2.tar.bz2** desde **www.phppgadmin.org** , lo copiamos al directorio **DocumentRoot** de apache que generalmente es **/var/www**, lo descomprimimos y le cambiamos de nombre

```
cp phpPgAdmin-4.2.tar.bz2 /var/www/
cd /var/www/
tar jxvf  phpPgAdmin-4.2.tar.bz2
mv phpPgAdmin-4.2.tar.bz2 phpPgAdmin
```

Ahora editamos el archivo de configuración de phpPgAdmin

```
vim phpPgAdmin/conf/config.inc.php
```

y modificamos lo siguiente

```
$conf['servers'][0]['host'] =
'localhost';
$conf['servers'][0]['pg_dump_path'] =
'/home/postgres/pgsql/bin/pg_dump';
$conf['servers'][0]['pg_dumpall_path'] =
'/home/postgres/pgsql/bin/pg_dumpall';
$conf['extra_login_security'] = false
```

Podemos configurar nuestro archivo **httpd.conf** de la siguiente manera

```
williams@TuX: ~
NameVirtualHost 127.0.0.1:80

<VirtualHost phppgadmin:80>
        ServerName phppgadmin
        DocumentRoot "/var/www/phpPgAdmin"
        DirectoryIndex index.php
</VirtualHost>

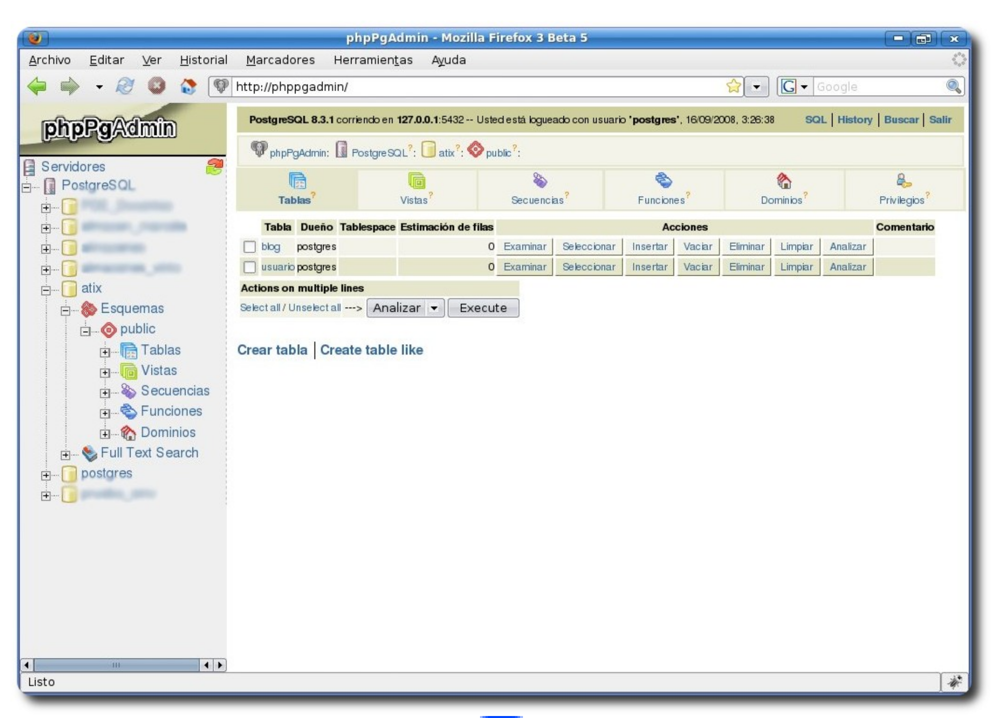
<VirtualHost localhost>
        ServerName localhost
        DocumentRoot "/var/www/"
        DirectoryIndex index.php
</VirtualHost>

```

y añadiendo la siguiente linea al inicio del archivo **/etc/hosts**

```
127.0.0.1     phppgadmin
```

ahora nos tendremos que dirigir a la siguiente ruta en nuestro navegador : **http://phppgadmin/**



y podremos disfrutar de un entorno gráfico desde donde podremos manejar postgreSQL no olviden que solo tienen que suministrar la cuenta y no así la contraseña de nuestro usuario.

PGAdmin 3

Esta es otra excelente herramienta con la cual podemos realizar la administración de nuestro Servidor, lo pueden encontrar en el repositorio de su distribución y es el que viene por defecto en el instalador de postgresql para window$ también lo pueden instalar desde sus fuentes pero en nuestro caso no olviden añadir el parámetro **`–with-pgsql=$PGHOME`** que en nuestro caso es **`/home/postgres/data/pgsql`** por lo demás no tendrían problemas.

La primera vez que arranquen pgadmin3 se les presentará una ventana como la siguiente:



En la cual tienen que proporcionar un nombre para su conexión al servidor cualquier nombre esta bien, además de el IP a donde se van a conectar en nuestro caso como es servidor esta en nuestro equipo con localhost tenemos suficiente, la cuenta con la cual nos vamos a conectar, si quieren pueden almacenar el password en caso de que tuvieran alguno esto para evitar que les pida password cada vez que quieren conectarse.

Una vez proporcionado estos datos y conectados a la base de datos tendremos una ventana similar a la siguiente:

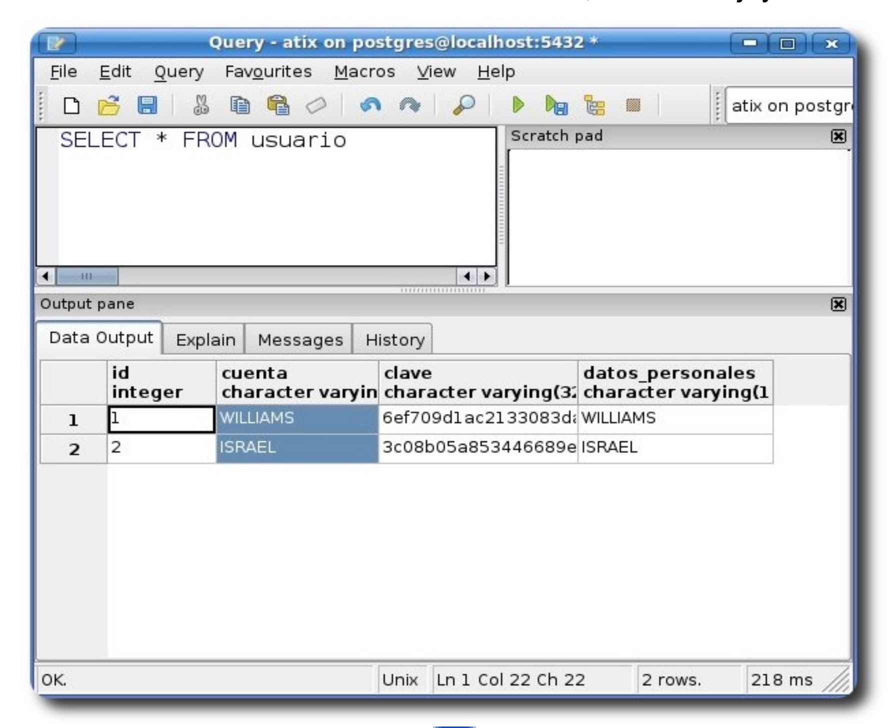
Property	Value
Name	usuario
OID	33862
Owner	postgres
Tablespace	pg_default
ACL	
Primary key	id
Rows (estimated)	0

```
-- Table: usuario

-- DROP TABLE usuario;

CREATE TABLE usuario
(
  id integer NOT NULL DEFAULT nextval('usuario_seq'::regclass),
  cuenta character varying(15),
  clave character varying(32),
  datos_personales character varying(120),
  CONSTRAINT usuario_pk PRIMARY KEY (id),
  CONSTRAINT check_clave CHECK (length(btrim(clave::text)) > 0),
  CONSTRAINT check_cuenta CHECK (length(btrim(cuenta::text)) > 0),
  CONSTRAINT check_datos_personales CHECK (length(btrim(datos_personal
)
WITH (OIDS=FALSE);
ALTER TABLE usuario OWNER TO postgres;
```

Posee una Editor SQL muy bueno en el cual podemos ejecutar cualquier consulta con F5 también un analizador de consultas que nos indica cuales fueron los pasos llevados a cabo para obtener cada consulta Seleccionen la pestaña Explain y presionen F7 también podemos exportar el resultado de nuestras consultas a formato html, en fin una joyita.

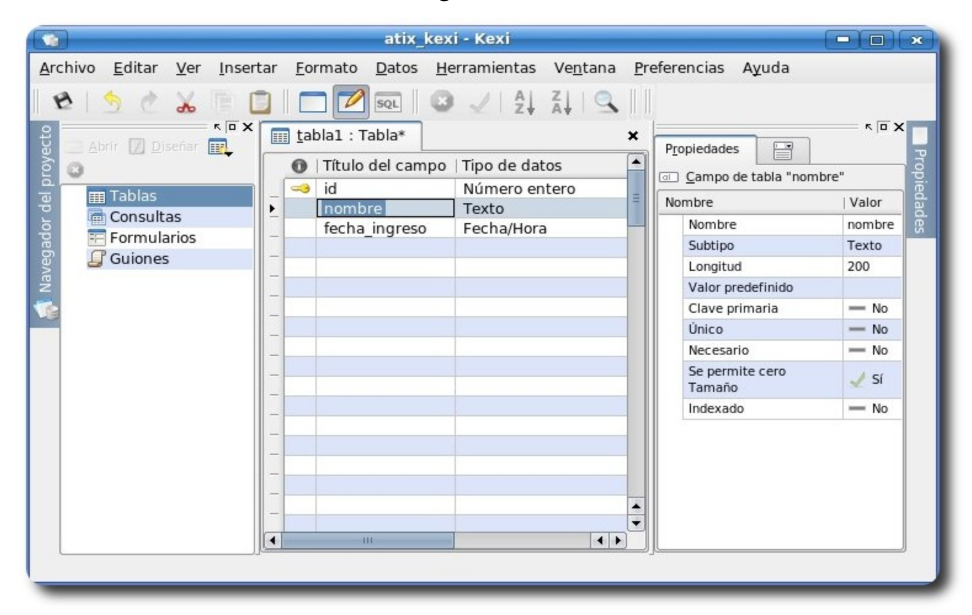


KEXI

Dentro del Suite de Ofimática de **KDE KOFFICE** encontramos esta herramienta que es mas o menos un clon de Access que también se puede conectar con PostgreSQL veamos lo primero que se nos presenta es una ventana en la cual seleccionamos Base de Datos Vacía y hacemos click en aceptar ahora el proyecto que nosotros queremos crear puede estar contenido en un archivo o en un servidor de Base de Datos (adivinen que opción vamos seleccionar) obviamente la Segunda.



Ahora tenemos que crear la conexión para lo cual hacemos click en el botón añadir a lo cual se nos presentará una nueva ventana de la cual seleccionamos el motor PostgreSQL (también se puede trabajar con MySql) y proporcionamos los datos de la cuenta y contraseña y un Título para la Base de Datos (es opcional) podemos probar la conexión, luego presionamos añadir ahora hacemos click en el botón siguiente y damos un nuevo nombre a nuestro proyecto y a la base de datos por ejemplo atix_kexi y finalmente hacemos click en crear. Desde aquí podremos crear las tablas, formularios todo muy similar al software que mencione al inicio. Una opción interesante dentro de los front-ends de PostgreSQL



OpenOffice - Base

Finalmente Dentro de la Suite Ofimática OpenOffice podemos encontrar Base la cual tengo entendido se puede conectar a PostgreSQL a través de ODBC.

Curiosidades

Navegando por internet encontré una entrada titulada 10 cosas para comenzar a usar Postgresql aunque en algunos puntos puedes ser muy genérico, pero es muy interesante de la cual extraigo algunos, de todas formas pueden acceder al articulo de forma completa en **http://www.midstorm.org/~telles/2006/09/10/10-dicas-para-comecar-a-usar-o-postgresql/**

1. Aprender Ingles (aunque esto es importante para todo)
2. Tratar de Resolver un problema real no importa lo pequeño que este sea.
3. Primero que nada consulte la Documentación del SGBD, y PostgreSQL cuenta con un muy buena documentación unas 2034 páginas que son de mucha ayuda.
4. Primero aprender a moverse en la consola ya de PostgreSQL psql o Mysql ayuda a conocer mas profundamente el SGDB que estamos manejando luego no tendremos problemas en usar un front-ent que nos facilite todo.
5. Procura participar en alguna comunidad de Software Libre afortunadamente hoy en día existe como mínimo uno en cada departamento de nuestro querido País así que busca una comunidad y apoya al movimiento del Software Libre.
6. Conoce tus capacidades como también tus limitaciones como también la de las Herramientas que usas.

Si bien hay mucho que escribir y también aprender sobre el manejo de PostgreSQL y su configuración, lo dejaremos hasta aquí por el momento, espero que les haya interesado usar PostgreSQL si tienen algunas dudas, consejos o sugerencias no duden en escribirme. Espero tener una nueva oportunidad para seguir hablando sobre PostgreSQL y sobre Software Libre en General.

Despedida

Finalmente esperar días mejores para nuestro País, que en este momento se encuentra en una situación difícil, solo de nosotros depende que nuestra patria salga adelante, así que todos pongamos nuestro granito de arena y **VIVA BOLIVIA!!!**

Referencias

[1] http://www.postgresql.org

Autor



Williams Israel Chorolque Choque
Egresado de la carrera de Ingeniería Informática
email: williamsis@gmail.com
Williams Israel Chorolque Choque

GNU Privacy Guard Intercambiando mensajes y documentos de forma segura

El intercambio de mensajes y documentos de forma segura hoy por hoy han cobrado un alto grado de importancia, sobre todo al momento de transferir mensajes o documentos por redes inseguras (Internet), por tal razón se debe hacer uso de herramientas y mencanismos que nos brinden la mayor seguridad posible.

Introducción

Hoy en día es bastante común escuchar frases como: "Me han pinchado el correo electrónico", "mis mensajes confidenciales dejan de serlo al enviarlos por Internet", "mis documentos son transformados y accedidos por personas desconocidas"; frases que se vierten principalmente en empresas que precisan mantener cierto grado de confidencialidad e integridad de la información que manejan e intercambian.

Este fenómeno no deja de estar exento en centros de investigación y desarrollo tecnológico, donde la confidencialidad y la integridad de la información que se maneja e intercambia son imprescindibles, es así que en este artículo trataremos de explicar las herramientas que nos permitirán realizar un intercambio de información de forma segura y confiable.

Firma digital

La firma digital o firma electrónica es, en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje.

La firma electrónica, como la firma hológrafa (autógrafa, manuscrita), puede vincularse a un documento para identificar al autor, para señalar conformidad (o disconformidad) con el contenido, para indicar que se ha leído o, según el tipo de firma, garantizar que no se pueda modificar su contenido.

La firma digital de documentos

La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido, y seguidamente aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma electrónica o digital.

La herramienta software que permita realizar la firma digital deberá realizar acciones como:

- ✔ Vigencia del certificado digital del firmante,
- ✔ Revocación del certificado digital del firmante (puede ser por OCSP o CRL),
- ✔ Inclusión de sello de tiempo.

Función hash

La función hash es un algoritmo matemático que permite calcular un valor resumen de los datos a ser firmados digitalmente, funciona en una sola dirección, es decir, no es posible a partir del valor resumen calcular los datos originales. Cuando la entrada es un documento, el resultado de la función es un número que identifica inequívocamente al texto. Si se adjunta este número al texto, el destinatario puede aplicar de nuevo la función y comprobar su resultado con el que ha recibido. No obstante éste tipo de operaciones no están pensadas para que las lleve a cabo el usuario, sino que se utiliza una herramienta software que automatiza tanto la función de calcular el valor hash como su verificación posterior.

GPG (GNU Privacy Guard)

Es una herramienta software de encriptación utilizado para cifrar y firmar mensajes y documentos digitales, que utiliza criptografía híbrida: combina criptografía simétrica (por su rapidez), con criptografía asimétrica (por no necesitar compartir claves secretas).

Viene a ser un remplazo del **PGP (Pretty Good Privacy)** pero con la principal diferencia que es software libre licenciado bajo la GPL. GPG utiliza el estándar del IETF denominado OpenPGP.

Claves públicas y privadas

GnuPG usa un sistema de claves públicas lo que quiere decir que cada usuario tiene una clave privada y una clave pública.

- ✔ La clave privada es la que se usa para desencriptar aquello que nos envían encriptado con nuestra clave pública, La clave privada es una clave que solo debe conocer el propietario ya que si ésta es comprometida o conocida por terceros estos podrán desencriptar los documentos y mensajes que se ha encriptado con nuestra clave pública.
- ✔ La clave pública es la que compartimos con las personas, para que éstas hagan uso de ésta para enviarnos mensajes o documentos encriptados.

Tipos de encriptación

Existen dos tipos:

- ✔ El simétrico : El encriptado simétrico consiste en que ambos extremos de la comunicación tienen la llave codificadora/decodificadora. Por la facilidad que estas llaves pueden ser comprometidas es la menos recomendada.
- ✔ El Asimétrico : El encriptado asimétrico consiste en el uso de dos llaves: Una llave pública de codificación, y una llave privada de decodificación. El extremo A envía su llave pública al extremo B, de tal forma que el extremo B le envíe mensajes codificados que sólo el extremo A puede decodificar usando su llave privada.

La decodificación de un mensaje o documento electrónico solo puede ser realizado utilizando la llave privada.

Qué puedo hacer con GnuPG

- ✔ Crear llaves públicas y privadas
- ✔ Administrar las llaves públicas
- ✔ Codificar datos usando las llaves públicas
- ✔ Decodificar datos usando las llaves privadas

Que preciso para hacer uso de GNUPG

Hoy por hoy todas las distribuciones de GNU/ Linux tienen la posibilidad de hacer uso de ésta herramienta, en muchos casos viene instalada por defecto, caso contrario podríamos hacer uso de utilidades como YUM o APT-GET para proceder a instalarlas según corresponda la distribución.

Procedimiento para encriptar mensajes y/o documentos electrónicos

Fundamentalmente deberíamos realizar las siguientes tareas:

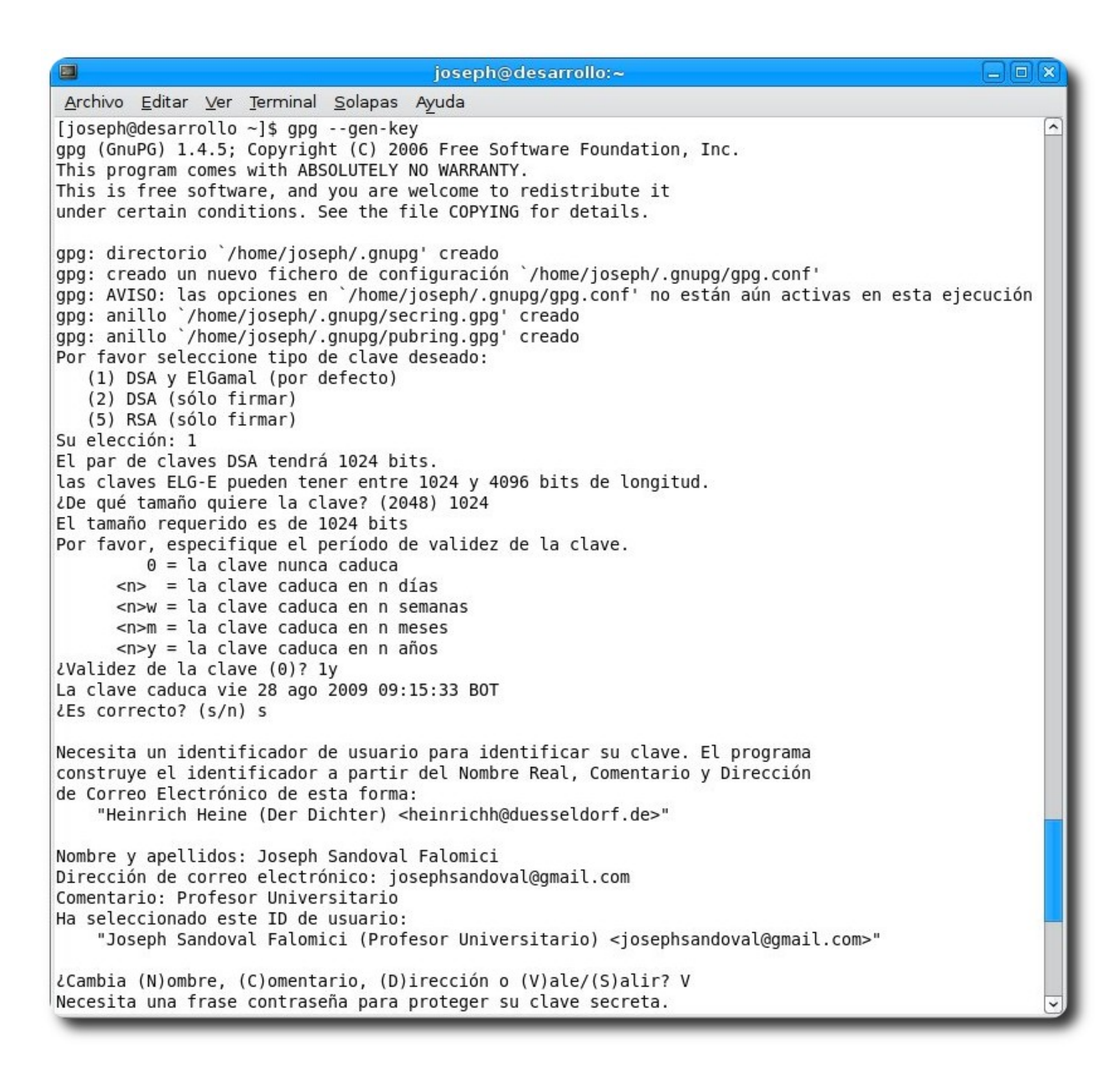
- ✔ Generar las llaves
- ✔ Exportar llaves
- ✔ Importar llaves
- ✔ Listar llaves
- ✔ Generar certificado de revocación
- ✔ Verificar firma de llaves
- ✔ Actualizar caducidad de llaves

Generar claves

En la generación de claves se debe especificar elementos como:

- ✔ Tipo de algoritmos de clave pública: DSA+ElGamal, DSA, ElGamal
- ✔ Longitud de clave
- ✔ Fecha de caducidad
- ✔ Identificación del usuario de las claves: nombre, e-mail,...
- ✔ "Frase secreta" para el acceso a las claves privadas (se pedirá para descifrar y firmar)

Tal como se muestra en la figura:



```
joseph@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/consola, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
..+++++.++++++++++++++.+++++.++++++++++.+++++++++++++++++++++++.++++++++++.++++++++++++++.++++
+++++++++++..++++++++++++++++++++++++.+++++>++++++++++........................+++++
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/consola, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
+++++++++++++++++++++++++++++.+++++++++++++++++++++++++++++++++++...++++++++++..++++++++++++++.+
++++++++++++++++++++++++++++++++++++++>+++++>..+++++.........................+++++^^^
gpg: /home/joseph/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: clave 8EAF7590 marcada como de confianza absoluta
claves pública y secreta creadas y firmadas.

gpg: comprobando base de datos de confianza
gpg: 3 dudosa(s) necesarias, 1 completa(s) necesarias,
modelo de confianza PGP
gpg: nivel: 0  validez:   1  firmada:   0  confianza: 0-, 0q, 0n, 0m, 0f, 1u
gpg: siguiente comprobación de base de datos de confianza el: 2009-08-28
pub   1024D/8EAF7590 2008-08-28 [caduca: 2009-08-28]
      Huella de clave = 062F B0A1 D442 9936 6F49  8ED5 70CD CF95 8EAF 7590
uid                  Joseph Sandoval Falomici (Profesor Universitario) <josephsandoval@gmail.com>
sub   1024g/FA6F4B98 2008-08-28 [caduca: 2009-08-28]

[joseph@desarrollo ~]$
```

```
joseph@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[joseph@desarrollo ~]$ gpg --gen-key
gpg (GnuPG) 1.4.5; Copyright (C) 2006 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

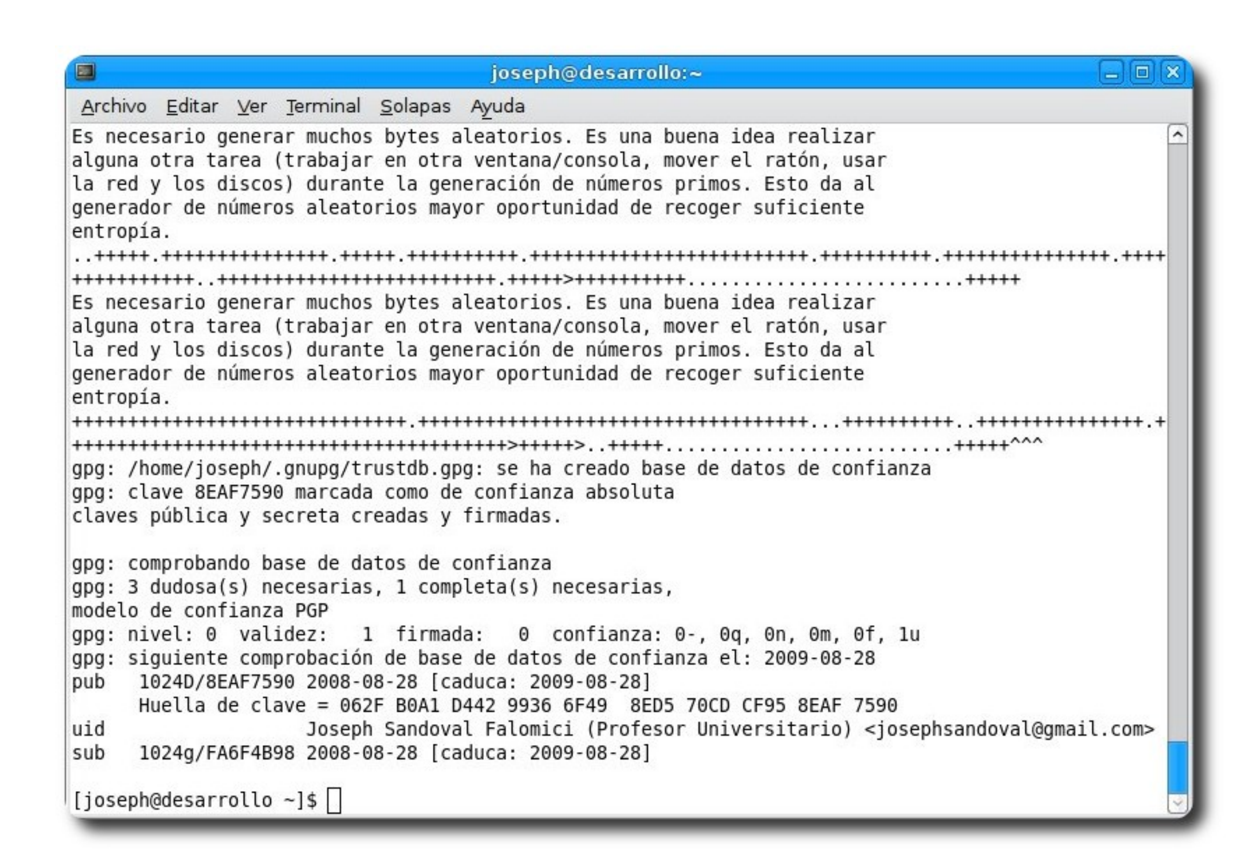
gpg: directorio `/home/joseph/.gnupg' creado
gpg: creado un nuevo fichero de configuración `/home/joseph/.gnupg/gpg.conf'
gpg: AVISO: las opciones en `/home/joseph/.gnupg/gpg.conf' no están aún activas en esta ejecución
gpg: anillo `/home/joseph/.gnupg/secring.gpg' creado
gpg: anillo `/home/joseph/.gnupg/pubring.gpg' creado
Por favor seleccione tipo de clave deseado:
   (1) DSA y ElGamal (por defecto)
   (2) DSA (sólo firmar)
   (5) RSA (sólo firmar)
Su elección: 1
```

```
joseph@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
El par de claves DSA tendrá 1024 bits.
las claves ELG-E pueden tener entre 1024 y 4096 bits de longitud.
¿De qué tamaño quiere la clave? (2048) 1024
El tamaño requerido es de 1024 bits
Por favor, especifique el período de validez de la clave.
         0 = la clave nunca caduca
      <n>  = la clave caduca en n días
      <n>w = la clave caduca en n semanas
      <n>m = la clave caduca en n meses
      <n>y = la clave caduca en n años
¿Validez de la clave (0)? 1y
La clave caduca vie 28 ago 2009 09:15:33 BOT
¿Es correcto? (s/n) s
```

```
joseph@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
Necesita un identificador de usuario para identificar su clave. El programa
construye el identificador a partir del Nombre Real, Comentario y Dirección
de Correo Electrónico de esta forma:
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Nombre y apellidos: Joseph Sandoval Falomici
Dirección de correo electrónico: josephsandoval@gmail.com
Comentario: Profesor Universitario
Ha seleccionado este ID de usuario:
    "Joseph Sandoval Falomici (Profesor Universitario) <josephsandoval@gmail.com>"

¿Cambia (N)ombre, (C)omentario, (D)irección o (V)ale/(S)alir? V
Necesita una frase contraseña para proteger su clave secreta.
```



```
joseph@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/consola, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
..+++++.+++++++++++++++.+++++.++++++++++.+++++++++++++++++++++++++.++++++++++.+++++++++++++++.++++
+++++++++++..+++++++++++++++++++++++++.+++++>++++++++++........................+++++
Es necesario generar muchos bytes aleatorios. Es una buena idea realizar
alguna otra tarea (trabajar en otra ventana/consola, mover el ratón, usar
la red y los discos) durante la generación de números primos. Esto da al
generador de números aleatorios mayor oportunidad de recoger suficiente
entropía.
++++++++++++++++++++++++++++++.+++++++++++++++++++++++++++++++++++...++++++++++..+++++++++++++++.+
++++++++++++++++++++++++++++++++++++++++>+++++>..+++++.........................+++++^^^
gpg: /home/joseph/.gnupg/trustdb.gpg: se ha creado base de datos de confianza
gpg: clave 8EAF7590 marcada como de confianza absoluta
claves pública y secreta creadas y firmadas.

gpg: comprobando base de datos de confianza
gpg: 3 dudosa(s) necesarias, 1 completa(s) necesarias,
modelo de confianza PGP
gpg: nivel: 0  validez:   1  firmada:   0  confianza: 0-, 0q, 0n, 0m, 0f, 1u
gpg: siguiente comprobación de base de datos de confianza el: 2009-08-28
pub   1024D/8EAF7590 2008-08-28 [caduca: 2009-08-28]
      Huella de clave = 062F B0A1 D442 9936 6F49  8ED5 70CD CF95 8EAF 7590
uid                  Joseph Sandoval Falomici (Profesor Universitario) <josephsandoval@gmail.com>
sub   1024g/FA6F4B98 2008-08-28 [caduca: 2009-08-28]

[joseph@desarrollo ~]$
```

Al generar las llaves por primera vez se crean los siguientes archivos



```
joseph@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayu
[joseph@desarrollo ~]$ tree .gnupg/
.gnupg/
|-- gpg.conf
|-- pubring.gpg
|-- pubring.gpg~
|-- random_seed
|-- secring.gpg
`-- trustdb.gpg

0 directories, 6 files
[joseph@desarrollo ~]$
```

Generar certificados de revocación de clave pública

Como precaución es posible que a futuro se desee invalidar las claves que se crearon, las posibles causas para esto podrían ser:

- ✔ Que tanto la frase de paso y el archivo con la clave privada hayan sido comprometidas lo que conduciría a la posibilidad que puedan suplantar nuestra identidad.
- ✔ Algo trivial pero que no se debe descartar es el olvido de la frase de paso, lo que impediría hacer uso de la clave privada para firmar mensajes o documentos.

Para cualquiera de estos casos u otros, se recomienda generar un certificado de revocación de la clave, ésta generación es preferible realizarla después de la generación de claves para evitar olvidar la frase de paso, aspecto que imposibilitaría crear el certificado de revocación.

Cuando el caso así lo amerite se recomienda propagar de forma fiable el certificado de revocación para proceder a inhabilitar las claves creadas anteriormente.

```
joseph@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[joseph@desarrollo ~]$ gpg --output certificado_revocacion.asc --gen-revoke 8EAF7590

sec  1024D/8EAF7590 2008-08-28 Joseph Sandoval Falomici (Profesor Universitario) <josephsandoval@gmail.com>

¿Crear un certificado de revocación para esta clave? (s/N) s
Por favor elija una razón para la revocación:
  0 = No se dio ninguna razón
  1 = La clave ha sido comprometida
  2 = La clave ha sido reemplazada.
  3 = La clave ya no está en uso
  Q = Cancelar
(Probablemente quería seleccionar 1 aquí)
¿Su decisión? 1
Introduzca una descripción opcional; acábela con una línea vacía:
> Mi clave ha sido sustraida y por ende comprometida
>
Razón para la revocación: La clave ha sido comprometida
Mi clave ha sido sustraida y por ende comprometida
¿Es correcto? (s/N) s

Necesita una frase contraseña para desbloquear la clave secreta
del usuario: "Joseph Sandoval Falomici (Profesor Universitario) <josephsandoval@gmail.com>"
clave DSA de 1024 bits, ID 8EAF7590, creada el 2008-08-28

se fuerza salida con armadura ASCII.
Certificado de revocación creado.

Por favor consérvelo en un medio que pueda esconder; si alguien consigue
acceso a este certificado puede usarlo para inutilizar su clave.
Es inteligente imprimir este certificado y guardarlo en otro lugar, por
si acaso su medio resulta imposible de leer. Pero precaución: ¡el sistema
de impresión de su máquina podría almacenar los datos y hacerlos accesibles
a otras personas!
[joseph@desarrollo ~]$
```

El contenido del certificado de revocación tiene esta apariencia.

```
joseph@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[joseph@desarrollo ~]$ cat certificado_revocacion.asc
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.5 (GNU/Linux)
Comment: A revocation certificate should follow

iHsEIBECADsFAki2sBE0HQJNaSBjbGF2ZSBoYSBzaWRvIHN1c3RyYWlkYSB5IHBv
ciBlbmRlIGNvbXByb21ldGlkYQAKCRBwzc+Vjq91kLYeAJ4x7I+TzJnewPcgKtgp
5nFy2IIeGgCdFkrv161IUMeeiX8wcPgrkb0oidY=
=ADLU
-----END PGP PUBLIC KEY BLOCK-----
[joseph@desarrollo ~]$
```

Exportar la clave pública propia

Antes de que se pueda usar la clave pública, por otras personas, se debe tener una copia de ésta. Para ello tiene que exportarla.

El exportar una clave pública representa volcarla a un fichero para distribuirlo a otros usuarios, para que puedan enviarnos mensajes y/o documentos cifrados con nuestra clave pública.

Puede guardarse en un fichero binario o en un fichero de texto con la opción **--armor**

```
joseph@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[joseph@desarrollo ~]$ gpg --armor --output joseph.gpg --export 8EAF7590
[joseph@desarrollo ~]$
```

Una clave exportada tiene la siguiente apariencia

```
joseph@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[joseph@desarrollo ~]$ cat joseph.gpg
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.5 (GNU/Linux)
```

```
mQGiBEi2pV4RBADCXh/EehAei2qhoJm1uJTJ6aJPwyG7fbwSZfSFV3ZVj6DEB1pl
rP/4Adlns2rB0nAfyYdPtbLEv+DJGVpNZ55CKSAb3eoSAXL8BnsBhOpSyFmP42Kg
wMt69jNOmIieDs9/N+PvkCj0KBYNBvnCJYkLmTjf9CpnfcsiwuP60BY0iwCg3BAb
xRlfEWSTB6Z9TiL0EyyQrbkD/0sA5135kAC2kIeAThjGvL2KvrfiPQ5R3AV2yeyQ
RHrH5RiOYKXKnKSCFUugeGyaY0GSH7GNEpF4Ztatb9S5L3Pl8vSes1+swCXu0sa+
MMr8jLWOTYwR63nepR30TYc3Jp2Ny9Mk1ynS9fTt2AqM+8fQ+zSPWj6g9gSULIYw
J6ADA/4/om1y6BSwE1SeGDn2Azi3BHl8F2q3Uwses+PZoitGI60B1SoteSmer0o1
drYOf3E0a82tJFDCNM5gjmS4Zp+l7qaVOTMgoYTh+kLfIQuzAnBrhmV3S85Mt4pl
9caryRmwKScQr1Kq/ncJZn13iEvD+fJ0mOYIBb2xMsGxxmOiH7RMSm9zZXBoIFNh
bmRvdmFsIEZhbG9taWNpIChQcm9mZXNvciBVbml2ZXJzaXRhcmlvKSA8am9zZXBo
c2FuZG92YWxAZ21haWwuY29tPohmBBMRAgAmBQJItqVeAhsDBQkB4TOABgsJCAcD
AgQVAggDBBYCAwECHgECF4AACgkQcM3PlY6vdZAmCwCfVVaXypdf6ohRfcCSF4k9
+kc1MiAAnjG60ijJ8KJFWlKMjQ6wapz2opxeuQENBEi2pV8QBADwdK2OTIUgVyXf
Eb+znHmYzbkun3ldL4qo6UWdJHWgqd9Nl7xACGm58sKhwzg3np6vhqlxQQp/prlW
7O5+X/tNUtYdg2QaqLnYcmnB1lBfjXyTgwSWizFkZU4t3/TwiaKtEY64V0zxvQWq
fTccCgndI/AvsA4Plg1t5vaNwAC+NwADBQP/aL3BDpyXOvPlxoOimDlgqkfE/OE1
L66gmx7FDnk/4XFM6nbFQOsq6ZCO4qKhyJo1HWUQty/HrA2FXYM7yRpgtxFb8OQm
AkcEKn4kJA+s8U95lHNBVsKP1lfKlAELaSvo3mtFe4nH/S56IlcwPjzilJx776V0
G9uA7nIffsVpwwaITwQYEQIADwUCSLalXwIbDAUJAeEzgAAKCRBwzc+Vjq91kBbQ
AJoDwLwfcfgXcVFjdbvZjrt5LRbIFACfYVown4K+SogDZZy6WRIERCsCCbU=
=LY66
```

```
-----END PGP PUBLIC KEY BLOCK-----
[joseph@desarrollo ~]$
```

Importar claves

Cada usuario puede disponer de una anillo de claves (análogo a un llavero), donde puede incluir (importar) claves públicas de otros usuarios. Para importar una clave podemos recurrir al archivo que contiene la misma o importarla desde un servidor de llaves para lo cual es preciso conocer el UID, en nuestro caso haremos la importación desde un archivo.

```
joseph@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[joseph@desarrollo ~]$ gpg --import esteban.gpg
gpg: clave 12D98C4B: clave pública "Esteban Saavedra Lopez (Director Revista ATIX) <estebansaavedra@gmail.com>" importada
gpg: Cantidad total procesada: 1
gpg:               importadas: 1
[joseph@desarrollo ~]$
```

Listar claves públicas

Para ver las llaves públicas que tenemos disponibles hacemos uso del comando **`gpg --list-keys`**. Esto listará las llaves que hay disponibles dentro del fichero **`pubring.gpg`**.

```
joseph@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[joseph@desarrollo ~]$ gpg --list-keys
/home/joseph/.gnupg/pubring.gpg
-------------------------------
pub   1024D/8EAF7590 2008-08-28 [caduca: 2009-08-28]
uid                  Joseph Sandoval Falomici (Profesor Universitario) <josephsandoval@gmail.com>
sub   1024g/FA6F4B98 2008-08-28 [caduca: 2009-08-28]

pub   1024D/12D98C4B 2008-08-28 [caduca: 2009-08-28]
uid                  Esteban Saavedra Lopez (Director Revista ATIX) <estebansaavedra@gmail.com>
sub   2048g/8B2B3465 2008-08-28 [caduca: 2009-08-28]

[joseph@desarrollo ~]$
```

Listar llaves privadas

Para ver las llaves privadas que tenemos disponibles hacemos uso del comando **`gpg --list-secret-keys`**. Esto listará las llaves que hay disponibles dentro del fichero **`secring.gpg`**.

```
joseph@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[joseph@desarrollo ~]$ gpg --list-secret-keys
/home/joseph/.gnupg/secring.gpg
-------------------------------
sec   1024D/8EAF7590 2008-08-28 [caduca: 2009-08-28]
uid                  Joseph Sandoval Falomici (Profesor Universitario) <josephsandoval@gmail.com>
ssb   1024g/FA6F4B98 2008-08-28

[joseph@desarrollo ~]$
```

Borrar claves de los anillos

Se llama anillos (llaveros) a los archivos en los que se guardan las claves públicas (**`pubring.gpg`**) y las privadas (**`secring.gpg`**). El orden que se debe seguir para su borrado es primeramente borrar las claves privadas y luego las públicas, ya que puede existir claves asociadas.

- ✔ Para borrar claves privadas se hace con el comando **`gpg --delete-secret-key ClaveID`**
- ✔ Para borrar claves públicas se hace con el comando **`gpg --delete-key ClaveID`**

```
joseph@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[joseph@desarrollo ~]$ gpg --delete-key 12D98C4B
gpg (GnuPG) 1.4.5; Copyright (C) 2006 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.


pub  1024D/12D98C4B 2008-08-28 Esteban Saavedra Lopez (Director Revista ATIX) <estebansaavedra@gmail.com>

¿Eliminar esta clave del anillo? (s/N) s
[joseph@desarrollo ~]$
```

Huella de la clave

Las claves están identificadas por una huella (fingerprint). La huella es una serie de números que se usa para verificar si una clave pertenece realmente al propietario. Se sugiere que al recibir una clave obtengamos su huella y la verifiquemos con la persona propietaria de la clave (para verificar si es correcta o ha sido manipulada). La huella es como aplicar un checksum de un fichero para verificar la integridad del mismo.

Al observar la huella podemos hacer uso de cualquier dato que identifique a la clave en cuestión (nombre, email, descripción o parte de ellas)

```
joseph@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[joseph@desarrollo ~]$ gpg --fingerprint 8EAF7590
pub   1024D/8EAF7590 2008-08-28 [caduca: 2009-08-28]
      Huella de clave = 062F B0A1 D442 9936 6F49  8ED5 70CD CF95 8EAF 7590
uid                  Joseph Sandoval Falomici (Profesor Universitario) <josephsandoval@gmail.com>
sub   1024g/FA6F4B98 2008-08-28 [caduca: 2009-08-28]

[joseph@desarrollo ~]$
```

También tenemos la posibilidad de usar un conjunto de caracteres, los cuales pueden identificar a varias claves.

```
joseph@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[joseph@desarrollo ~]$ gpg --fingerprint sa
pub   1024D/8EAF7590 2008-08-28 [caduca: 2009-08-28]
      Huella de clave = 062F B0A1 D442 9936 6F49  8ED5 70CD CF95 8EAF 7590
uid                  Joseph Sandoval Falomici (Profesor Universitario) <josephsandoval@gmail.com>
sub   1024g/FA6F4B98 2008-08-28 [caduca: 2009-08-28]

pub   1024D/12D98C4B 2008-08-28 [caduca: 2009-08-28]
      Huella de clave = 03C7 2E16 5066 467A EE54  549C 67BA C991 12D9 8C4B
uid                  Esteban Saavedra Lopez (Director Revista ATIX) <estebansaavedra@gmail.com>
sub   2048g/8B2B3465 2008-08-28 [caduca: 2009-08-28]

[joseph@desarrollo ~]$
```

Cifrado de ficheros

El cifrado de un documento da como resultado un archivo que está compuesto de la clave+el archivo cifrado.

Cuando ciframos un documento haciendo uso de una clave que no tiene una firma que garantice su autenticidad, obtenemos un mensaje de advertencia como se muestra en la figura:

```
esteban@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[esteban@desarrollo ~]$ gpg --armor --output articulo_cifrado.txt --recipient josephsandoval@gmail.com --encrypt articulo.pdf
gpg: FA6F4B98: No hay seguridad de que esta clave pertenezca realmente
al usuario que se nombra

pub  1024g/FA6F4B98 2008-08-28 Joseph Sandoval Falomici (Profesor Universitario) <josephsandoval@gmail.com>
 Huella de clave primaria: 062F B0A1 D442 9936 6F49  8ED5 70CD CF95 8EAF 7590
      Huella de subclave: AC79 215A C28A 3C6D 3F71  1D8C 922D 0F5B FA6F 4B98

No es seguro que la clave pertenezca a la persona que se nombra en el
identificador de usuario. Si *realmente* sabe lo que está haciendo,
puede contestar sí a la siguiente pregunta.

¿Usar esta clave de todas formas? (s/N) s
[esteban@desarrollo ~]$
```

Mientras que cuando ciframos un documento con una clave firmada, no tendremos ningún mensaje de advertencia, ya que se considera que si la clave está firmada es garantizada.

```
esteban@desarrollo:~
Archivo Editar Ver Terminal Solapas Ayuda
[esteban@desarrollo ~]$ gpg --armor --output resumen_cifrado.txt --recipient greghosalki@gmail.com --encrypt resumen.pdf
[esteban@desarrollo ~]$
```

Si deseamos que el archivo cifrado resultante no sea de tipo texto, debemos omitir el parámetro –**armor**, lo que permitirá obtener un archivo cifrado pero binario.

```
esteban@desarrollo:~
Archivo Editar Ver Terminal Solapas Ayuda
[esteban@desarrollo ~]$ gpg --output articulo.pdf.gpg --recipient greghosalki@gmail.com --encrypt articulo.pdf
[esteban@desarrollo ~]$
```

Descifrado de ficheros

El descifrado de un documento que haya sido cifrado en formato texto o binario, es análogo como muestran las siguientes figuras:

```
joseph@desarrollo:~
Archivo Editar Ver Terminal Solapas Ayuda
[joseph@desarrollo ~]$ gpg --output articulo.pdf --decrypt articulo_cifrado.txt

Necesita una frase contraseña para desbloquear la clave secreta
del usuario: "Joseph Sandoval Falomici (Profesor Universitario) <josephsandoval@gmail.com>"
clave ELG-E de 1024 bits, ID FA6F4B98, creada el 2008-08-28(ID de clave primaria 8EAF7590)

gpg: cifrado con clave ELG-E de 1024 bits, ID FA6F4B98, creada el 2008-08-28
      "Joseph Sandoval Falomici (Profesor Universitario) <josephsandoval@gmail.com>"
[joseph@desarrollo ~]$
```

```
gregory@desarrollo:~
Archivo Editar Ver Terminal Solapas Ayuda
[gregory@desarrollo ~]$ gpg --output articulo.pdf --decrypt articulo.pdf.gpg

Necesita una frase contraseña para desbloquear la clave secreta
del usuario: "Gregory Hosalki Jensen (Investigador) <greghosalki@gmail.com>"
clave ELG-E de 1024 bits, ID 66F5BC14, creada el 2008-08-28(ID de clave primaria 20A681F7)

gpg: cifrado con clave ELG-E de 1024 bits, ID 66F5BC14, creada el 2008-08-28
      "Gregory Hosalki Jensen (Investigador) <greghosalki@gmail.com>"
[gregory@desarrollo ~]$
```

Encriptado simétrico

Es posible encriptar archivos usando contraseñas en vez de claves. La contraseña funcionará como clave y será utilizada como encriptado simétrico

```
esteban@desarrollo:~
Archivo Editar Ver Terminal Solapas Ayuda
[esteban@desarrollo ~]$ gpg --output articulo.pdf.gpg --symmetric articulo.pdf
Repita frase contraseña:
```

Al momento de desencriptar, precisaremos conocer la contraseña con la que fue encriptado el documento.

```
gregory@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[gregory@desarrollo ~]$ gpg --output articulo.pdf --decrypt articulo.pdf.gpg
gpg: datos cifrados CAST5
gpg: cifrado con 1 frase contraseña
gpg: ATENCIÓN: la intgridad del mensaje no está protegida
[gregory@desarrollo ~]$
```

Firma digital

Al momento de intercambiar mensajes o documentos encriptados, es recomendable que los firmemos digitalmente, de esta forma evitaremos que cualquier persona que tenga una llave pública pueda suplantar a otra.

El intercambio de mensajes o documentos puede considerar: encriptado, firmado, encriptado y firmado

Firmado

El firmado de un documento puede dar como resultado un archivo binario, para nuestro ejemplo (**presentacion.pdf.gpg**) haciendo uso de la opción **--sign**

```
esteban@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[esteban@desarrollo ~]$ gpg --sign presentacion.pdf

Necesita una frase contraseña para desbloquear la clave secreta
del usuario: "Esteban Saavedra Lopez (Director Revista ATIX) <estebansaavedra@gmail.com>"
clave DSA de 1024 bits, ID 12D98C4B, creada el 2008-08-28

[esteban@desarrollo ~]$
```

o un archivo de tipo texto (**presentacion.pdf.asc**), haciendo uso de la opción **–clearsign**, para firmar el fichero encriptado en formato 7-bit ASCII.

```
esteban@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[esteban@desarrollo ~]$ gpg --clearsign presentacion.pdf

Necesita una frase contraseña para desbloquear la clave secreta
del usuario: "Esteban Saavedra Lopez (Director Revista ATIX) <estebansaavedra@gmail.com>"
clave DSA de 1024 bits, ID 12D98C4B, creada el 2008-08-28

[esteban@desarrollo ~]$
```

Encriptado + firmado

Para otorgarle mayor seguridad a la transferencia de mensajes o documentos podemos encriptarlos y firmarlos simultáneamente, como se muestra en la figura:

```
esteban@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[esteban@desarrollo ~]$ gpg --output presentacion.pdf.gpg --sign --recipient greghosalki@gmail.com --encrypt presentacion.pdf

Necesita una frase contraseña para desbloquear la clave secreta
del usuario: "Esteban Saavedra Lopez (Director Revista ATIX) <estebansaavedra@gmail.com>"
clave DSA de 1024 bits, ID 12D98C4B, creada el 2008-08-28

[esteban@desarrollo ~]$
```

Cuando desencriptamos un archivo que ha sido encriptado y firmado, el proceso nos informará de éste hecho, así como se muestra en la figura:

```
gregory@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[gregory@desarrollo ~]$ gpg --output presentacion.pdf --decrypt presentacion.pdf.gpg

Necesita una frase contraseña para desbloquear la clave secreta
del usuario: "Gregory Hosalki Jensen (Investigador) <greghosalki@gmail.com>"
clave ELG-E de 1024 bits, ID 66F5BC14, creada el 2008-08-28(ID de clave primaria 20A681F7)

gpg: cifrado con clave ELG-E de 1024 bits, ID 66F5BC14, creada el 2008-08-28
      "Gregory Hosalki Jensen (Investigador) <greghosalki@gmail.com>"
gpg: Firmado el jue 28 ago 2008 18:11:59 BOT usando clave DSA ID 12D98C4B
gpg: Firma correcta de "Esteban Saavedra Lopez (Director Revista ATIX) <estebansaavedra@gmail.com>"
[gregory@desarrollo ~]$
```

Verificando el firmado

Si hemos recibido un mensaje o documento firmado, debemos proceder a verificar la firma independientemente de como haya sido firmado, así como se muestra en las figuras siguientes:



Solo firmas acompañantes

Algunas veces nos puede interesar separar la firma del fichero original y generar un archivo adicional para la firma

```
esteban@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[esteban@desarrollo ~]$ gpg --armor --output firma_articulo.txt --detach-sign articulo.pdf


Necesita una frase contraseña para desbloquear la clave secreta
del usuario: "Esteban Saavedra Lopez (Director Revista ATIX) <estebansaavedra@gmail.com>"
clave DSA de 1024 bits, ID 12D98C4B, creada el 2008-08-28

[esteban@desarrollo ~]$
```

Al momento de verificar debemos tener tanto el archivo de firma como el archivo original, para que se realice la verificación correspondiente de asociación del archivo original como del archivo de firma

```
esteban@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[esteban@desarrollo ~]$ gpg --armor --output firma_articulo.txt --detach-sign articulo.pdf


Necesita una frase contraseña para desbloquear la clave secreta
del usuario: "Esteban Saavedra Lopez (Director Revista ATIX) <estebansaavedra@gmail.com>"
clave DSA de 1024 bits, ID 12D98C4B, creada el 2008-08-28

[esteban@desarrollo ~]$
```

Anillo de confianza

Un anillo de confianza consiste en firmar una clave de cierta persona de nuestra confianza o de quien podemos dar fe, con el objetivo de actuar como una especie de garantes de ésta. Una clave cuanto más firmas tenga se garantiza más la autenticidad de la misma y de la persona propietaria

Generalmente los anillos de confianza son utilizados para ingresar a ciertos grupos de investigación o desarrollo, análogamente como si un miembro antiguo garantizaría el ingreso de un miembro nuevo.

Cualquier usuario puede certificar una clave, pero existen instituciones que se dedican expresamente a la tarea de certificar claves públicas: son las llamadas Autoridades Certificadoras (**CA, Certificate Authority**), como **VeriSign, OpenCA, EnTrust**, etc.

```
esteban@desarrollo:~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
[esteban@desarrollo ~]$ gpg --sign-key 20A681F7

pub  1024D/20A681F7  creado: 2008-08-28  caduca: 2009-08-28  uso: SC
                     confianza: desconocido   validez: desconocido
sub  1024g/66F5BC14  creado: 2008-08-28  caduca: 2009-08-28  uso: E
[desconocida] (1). Gregory Hosalki Jensen (Investigador) <greghosalki@gmail.com>


pub  1024D/20A681F7  creado: 2008-08-28  caduca: 2009-08-28  uso: SC
                     confianza: desconocido   validez: desconocido
 Huella de clave primaria: CB21 8DFF 4AC7 1F5A 0CAE  BC30 A3B0 4610 20A6 81F7

     Gregory Hosalki Jensen (Investigador) <greghosalki@gmail.com>

Esta clave expirará el 2009-08-28.
¿Está realmente seguro de querer firmar esta clave
con su clave: "Esteban Saavedra Lopez (Director Revista ATIX) <estebansaavedra@gmail.com>" (12D98C4B)?

¿Firmar de verdad? (s/N) s

Necesita una frase contraseña para desbloquear la clave secreta
del usuario: "Esteban Saavedra Lopez (Director Revista ATIX) <estebansaavedra@gmail.com>"
clave DSA de 1024 bits, ID 12D98C4B, creada el 2008-08-28


[esteban@desarrollo ~]$
```

Si deseamos ver el listado de claves y cuales y por quienes están firmadas poder hacer uso del comando **`gpg --list-sigs`**

```
[esteban@desarrollo ~]$ gpg --list-sigs
/home/esteban/.gnupg/pubring.gpg
--------------------------------
pub   1024D/12D98C4B 2008-08-28 [caduca: 2009-08-28]
uid                  Esteban Saavedra Lopez (Director Revista ATIX) <estebansaavedra@gmail.com>
sig 3        12D98C4B 2008-08-28  Esteban Saavedra Lopez (Director Revista ATIX) <estebansaavedra@gmail.com>
sub   2048g/8B2B3465 2008-08-28 [caduca: 2009-08-28]
sig          12D98C4B 2008-08-28  Esteban Saavedra Lopez (Director Revista ATIX) <estebansaavedra@gmail.com>

pub   1024D/8EAF7590 2008-08-28 [caduca: 2009-08-28]
uid                  Joseph Sandoval Falomici (Profesor Universitario) <josephsandoval@gmail.com>
sig 3        8EAF7590 2008-08-28  Joseph Sandoval Falomici (Profesor Universitario) <josephsandoval@gmail.com>
sub   1024g/FA6F4B98 2008-08-28 [caduca: 2009-08-28]
sig          8EAF7590 2008-08-28  Joseph Sandoval Falomici (Profesor Universitario) <josephsandoval@gmail.com>

pub   1024D/20A681F7 2008-08-28 [caduca: 2009-08-28]
uid                  Gregory Hosalki Jensen (Investigador) <greghosalki@gmail.com>
sig 3        20A681F7 2008-08-28  Gregory Hosalki Jensen (Investigador) <greghosalki@gmail.com>
sig          12D98C4B 2008-08-28  Esteban Saavedra Lopez (Director Revista ATIX) <estebansaavedra@gmail.com>
sub   1024g/66F5BC14 2008-08-28 [caduca: 2009-08-28]
sig          20A681F7 2008-08-28  Gregory Hosalki Jensen (Investigador) <greghosalki@gmail.com>

[esteban@desarrollo ~]$
```

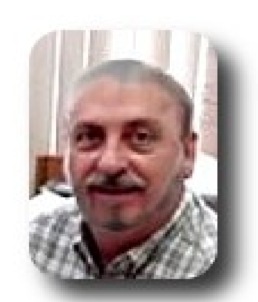
Referencias

[1] http://www.gnupg.org/

[2] http://es.wikipedia.com

Autores





Esteban Saavedra López
Líder de la Comunidad ATIX (Oruro – Bolivia)
Activista de Software Libre en Bolivia
jesaavedra@opentelematics.org
http://jesaavedra.opentelematics.org

Joseph Sandoval Falomici
Profesor universitario
Entusiasta de Software Libre
josephsandoval@gmail.com

Colaboración en las pruebas

Gregory Hosalki Jensen
Investigador (UK)
greghosalki@gmail.com

Interactuando con GNU Privacy Guard

El intercambio de mensajes y documentos de forma segura hoy por hoy han cobrado un alto grado de importancia, sobre todo al momento de transferir mensajes o documentos por redes inseguras (Internet), por tal razón se debe hacer uso de herramientas y mencanismos que nos brinden la mayor seguridad posible.



Introducción

En el artículo anterior observamos las grandes ventajas que pone a disposición el uso de GPG al momento de encriptar y/o firmar mensajes o documentos para ser transferidos o distribuidos a ciertos usuarios, dotándole de esta forma un alto nivel de seguridad.

En este artículo continuaremos mostrando más cualidades de GPG, también veremos temas relacionados como ser:

- ✔ El uso de la interfaz shell que nos permite interactuar con GPG
- ✔
- ✔ El uso de distintos frontends que permitirán que interactuemos de forma gráfica con GPG
- ✔ El uso de un servidor de claves, que nos permitirá publicar nuestras claves para que estas puedan ser obtenidas por otros usuarios.

GnuPG subshell

GnuPG nos provee la posibilidad de realizar algunos cambios en la clave desde la línea de comandos o por medio de una shell interactivo, que será el que veremos y demostraremos brevemente como funciona.

Para acceder a ésta shell hacemos uso del parámetro **`--edit-key`** acompañado de la UID. Las siguientes imágenes muestran algunas de las muchas posibilidades que se tiene en este shell interactivo.

```
esteban@desarrollo: ~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
esteban@desarrollo:~$ gpg --edit-key 12D98C4B
gpg (GnuPG) 1.4.6; Copyright (C) 2006 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

Clave secreta disponible.

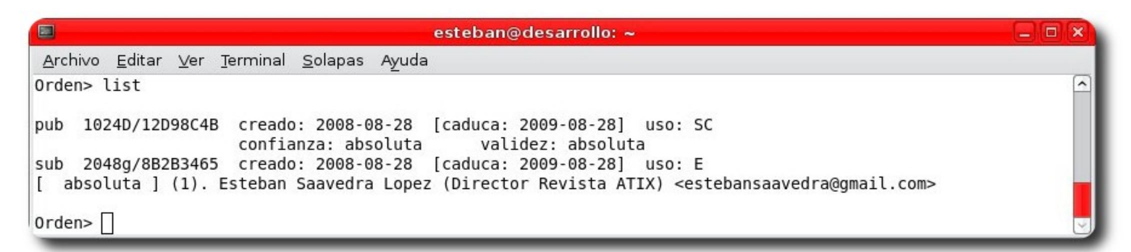
pub  1024D/12D98C4B  creado: 2008-08-28  [caduca: 2009-08-28]  uso: SC
                     confianza: absoluta      validez: absoluta
sub  2048g/8B2B3465  creado: 2008-08-28  [caduca: 2009-08-28]  uso: E
[  absoluta ] (1). Esteban Saavedra Lopez (Director Revista ATIX) <estebansaavedra@gmail.com>

Orden>
```

Ingreso al shell interactivo

```
esteban@desarrollo: ~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
Orden> ?
quit        Salir de este menú
save        graba y sale
help        Muestra esta ayuda
fpr         muestra huella dactilar
list        lista clave e identificadores de usuario
uid         selecciona identificador de usuario N
key         selecciona identificador de usuario N
check       revoca firmas
sign        firmar IDs seleccionadas [* ver debajo órdenes relacionadas]
lsign       firma la clave localmente
tsign       lid %lu: identificativo de usuario sin firma
nrsign      firmar IDs seleccionados con firma no revocable
adduid      añade un identificador de usuario
```

Listado de comandos disponibles



Listado de claves



Detalles del fingerprint



Firma de una clave

```
esteban@desarrollo: ~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
Orden> trust
pub  1024D/8EAF7590  creado: 2008-08-28  [caduca: 2009-08-28]  uso: SC
                     confianza: no definido   validez: total
sub  1024g/FA6F4B98  creado: 2008-08-28  [caduca: 2009-08-28]  uso: E
[   total   ] (1). Joseph Sandoval Falomici (Profesor Universitario) <josephsandoval@gmail.com>

Por favor, decida su nivel de confianza para que este usuario
verifique las claves de otros usuarios (mirando pasaportes,
comprobando huellas dactilares en diferentes fuentes...)

  1 = No lo sé
  2 = No confío
  3 = Confío poco
  4 = Confío totalmente
  5 = confío por completo
  m = volver al menú principal

Su decisión: 5
¿De verdad quiere asignar total confianza a esta clave? s
```

Niveles de confianza

```
esteban@desarrollo: ~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
Orden> check
uid  Joseph Sandoval Falomici (Profesor Universitario) <josephsandoval@gmail.com>
sig!3        8EAF7590 2008-08-28  [autofirma]
sig!         12D98C4B 2008-09-11  Esteban Saavedra Lopez (Director Revista ATIX)

Orden>
```

Detalles de una clave

```
esteban@desarrollo: ~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
Orden> expire
Cambiando caducidad de clave primaria.
Por favor, especifique el período de validez de la clave.
         0 = la clave nunca caduca
      <n>  = la clave caduca en n días
      <n>w = la clave caduca en n semanas
      <n>m = la clave caduca en n meses
      <n>y = la clave caduca en n años
¿Validez de la clave (0)? 5m
La clave caduca dom 08 feb 2009 12:28:58 BOT
¿Es correcto (s/n)? s

Necesita una frase contraseña para desbloquear la clave secreta
del usuario: "Esteban Saavedra Lopez (Director Revista ATIX) <estebansaavedra@gmail.com>"
clave DSA de 1024 bits, ID 12D98C4B, creada el 2008-08-28


pub  1024D/12D98C4B  creado: 2008-08-28  [caduca: 2009-02-08]  uso: SC
                     confianza: absoluta      validez: absoluta
sub  2048g/8B2B3465  creado: 2008-08-28  [caduca: 2009-08-28]  uso: E
[  absoluta ] (1). Esteban Saavedra Lopez (Director Revista ATIX) <estebansaavedra@gmail.com>

Orden>
```

Cambio de la fecha de expiración de la clave

```
esteban@desarrollo: ~
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
Orden> showpref
[  absoluta ] (1). Esteban Saavedra Lopez (Director Revista ATIX) <estebansaavedra@gmail.com>
     Cifrado: AES256, AES192, AES, CAST5, 3DES
     Resumen: SHA1, SHA256, RIPEMD160
     Compresión: ZLIB, BZIP2, ZIP, Sin comprimir
     Características: MDC, Sevidor de claves no-modificar

Orden>
```

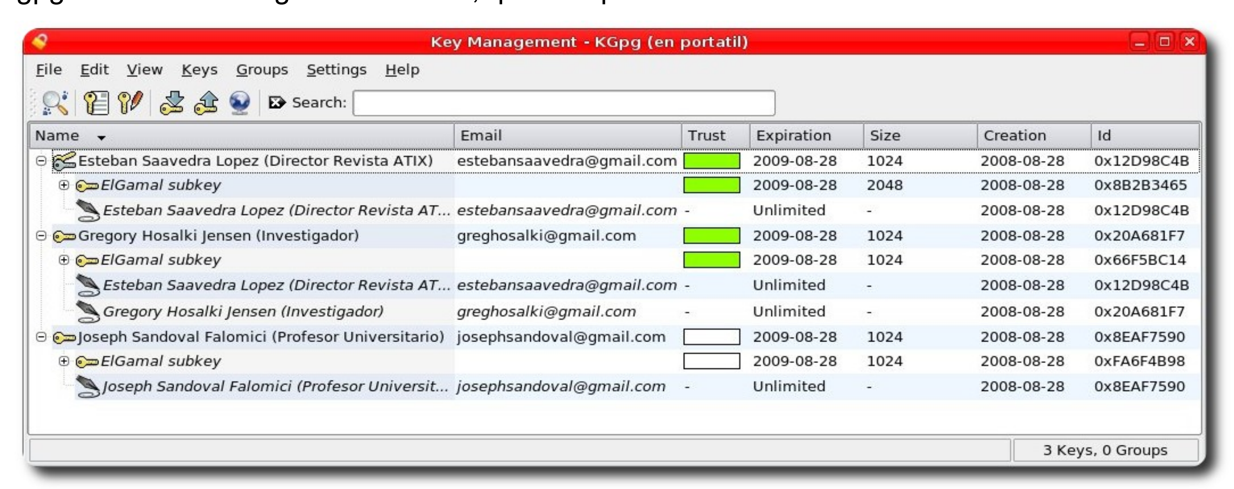
Preferencias de la clave

Interfaces gráficas

Actualmente disponemos de varias interfaces gráficas o frontends que nos permiten interactuar de forma un tanto más cómoda (dependiendo del usuario) con GPG, entre los que más destacan se encuentran KGPG,GPA y Seahorse.

KGPG

Kgpg es una interfaz gráfica de KDE, que nos permite interactuar con GPG.

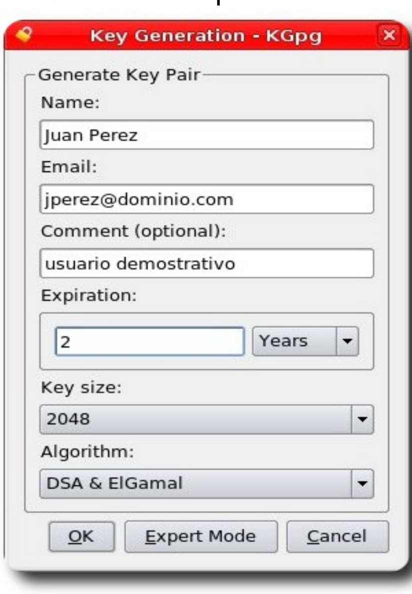


Listado de llaves



Detalles de una clave

Creación del par de claves





Notificación de la firma de una clave



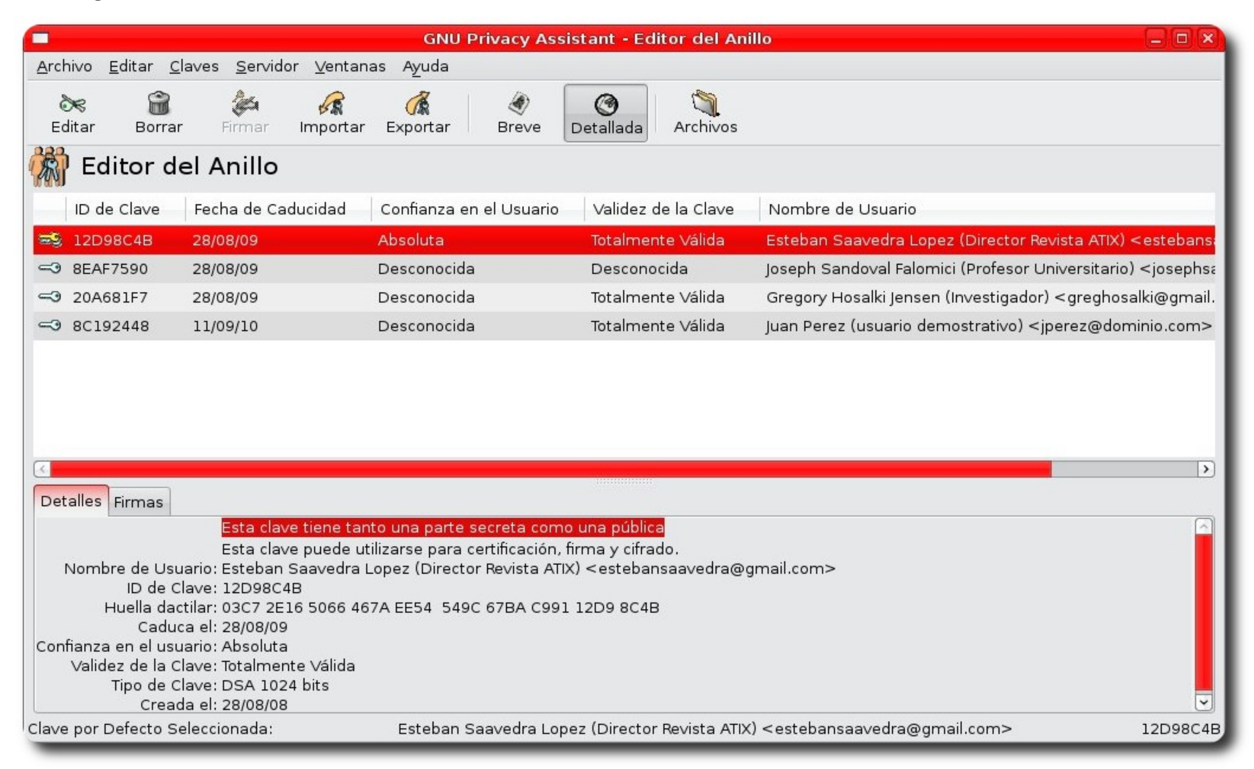
Exportación de claves



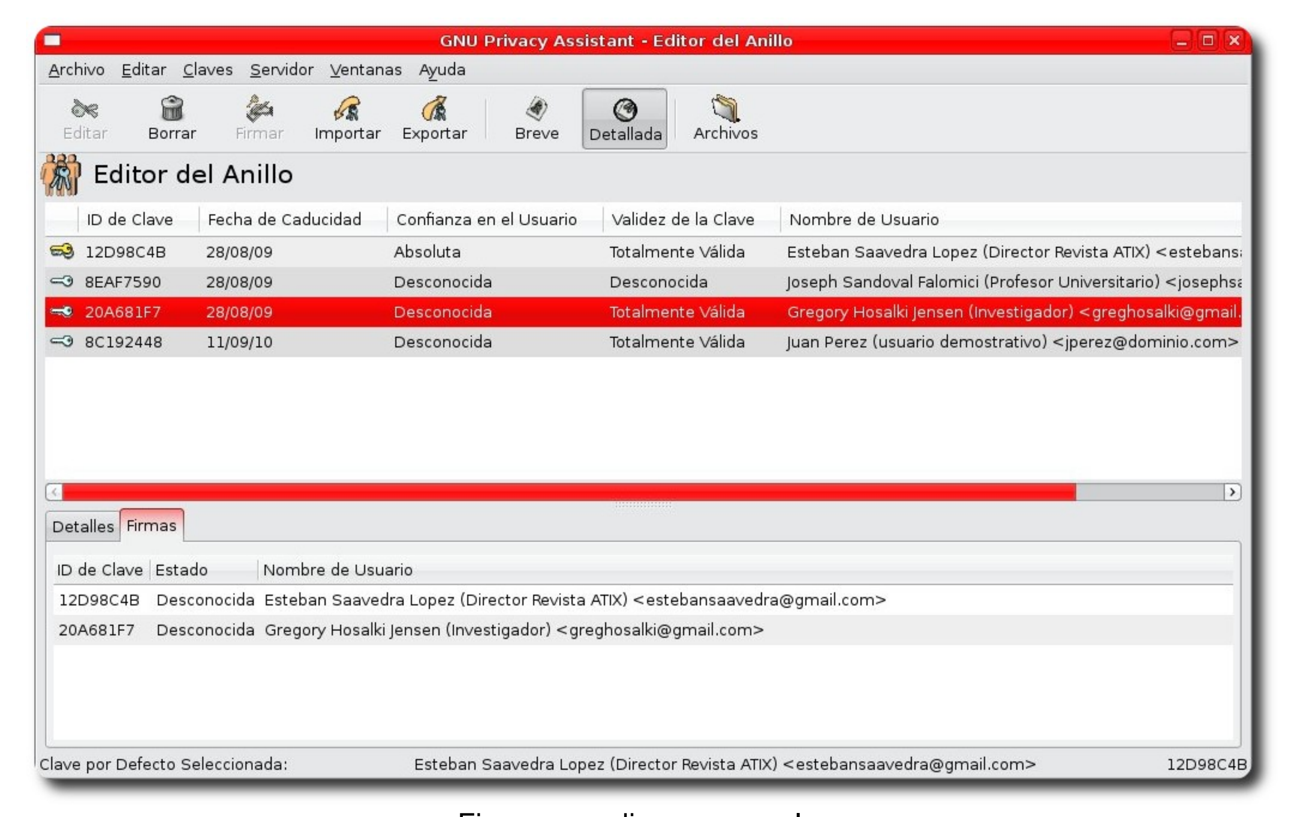
Configuración de servidores de claves públicos

GPA

GPA - The Gnu Privacy Assistant, es otra de las aplicaciones utilizadas para interactuar de forma gráfica con GPG.

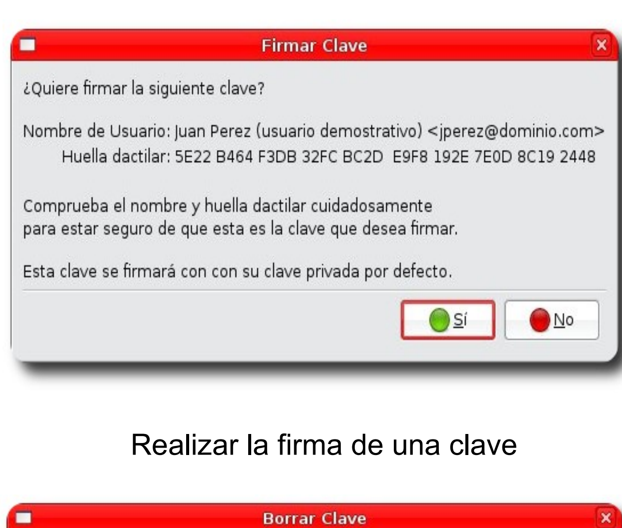


Detalles de una clave

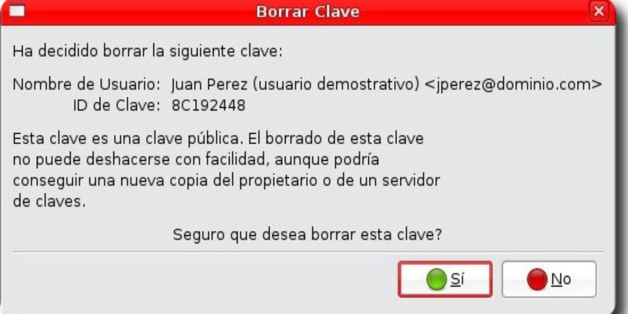


Firmas que dispone una clave

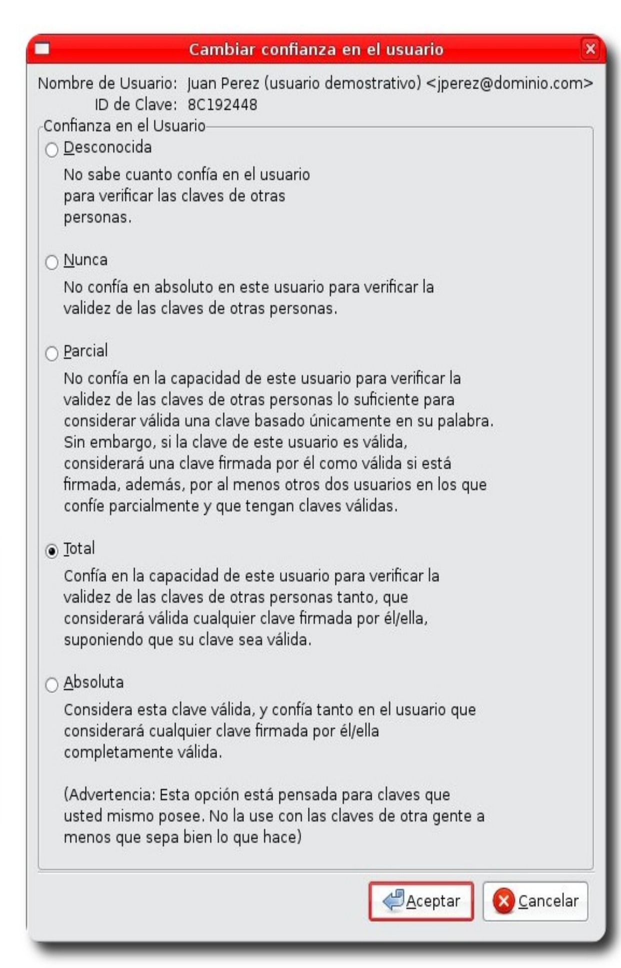




Realizar la firma de una clave



Borrado de una clave



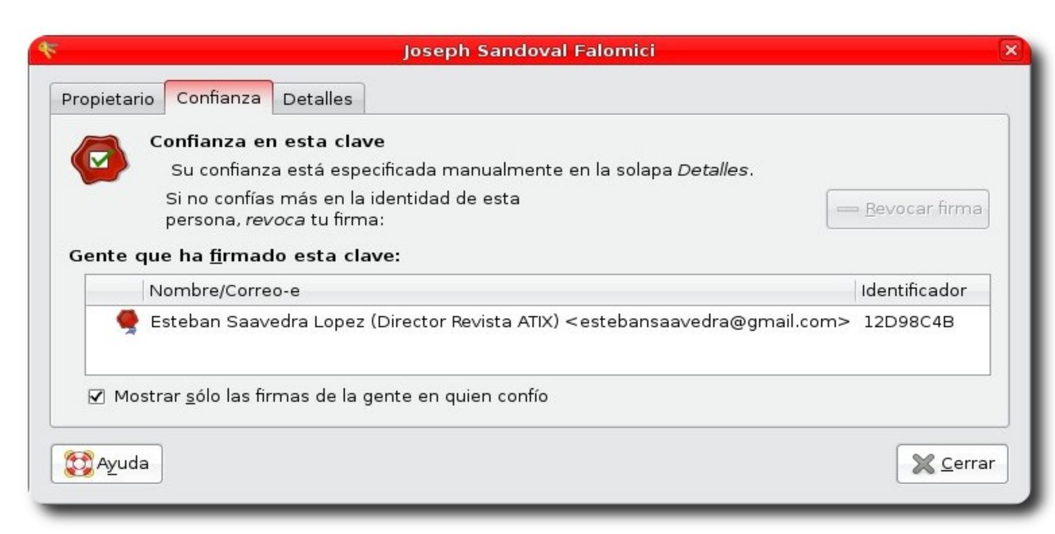
Niveles de confianza de una clave

Seahorse

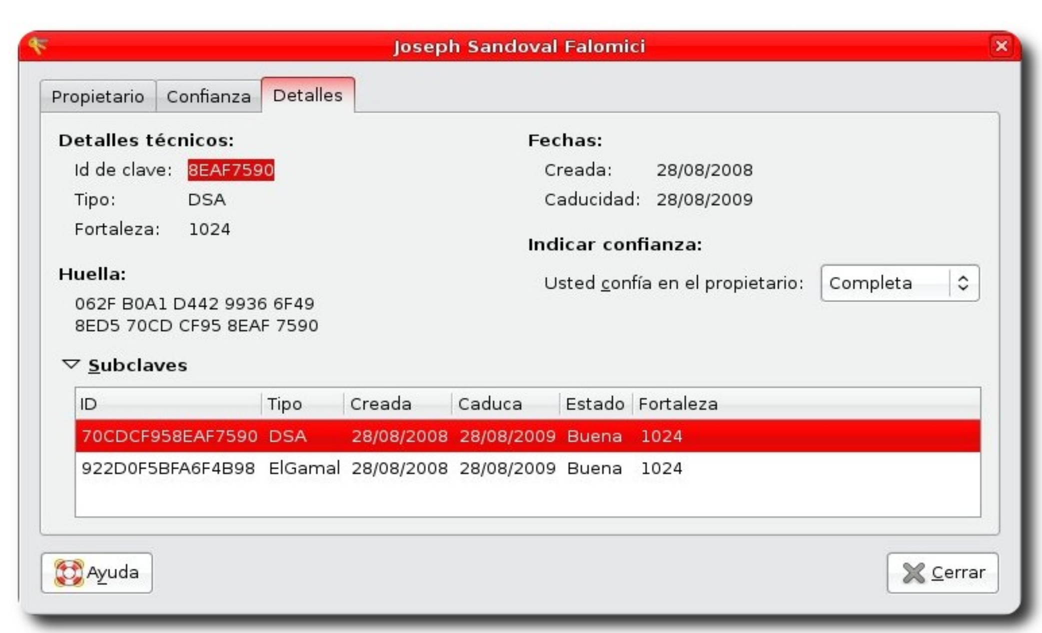
Seahorse al igual que las anteriores aplicaciones se han convertido en los frontends más utilizados para interactuar con GPG.



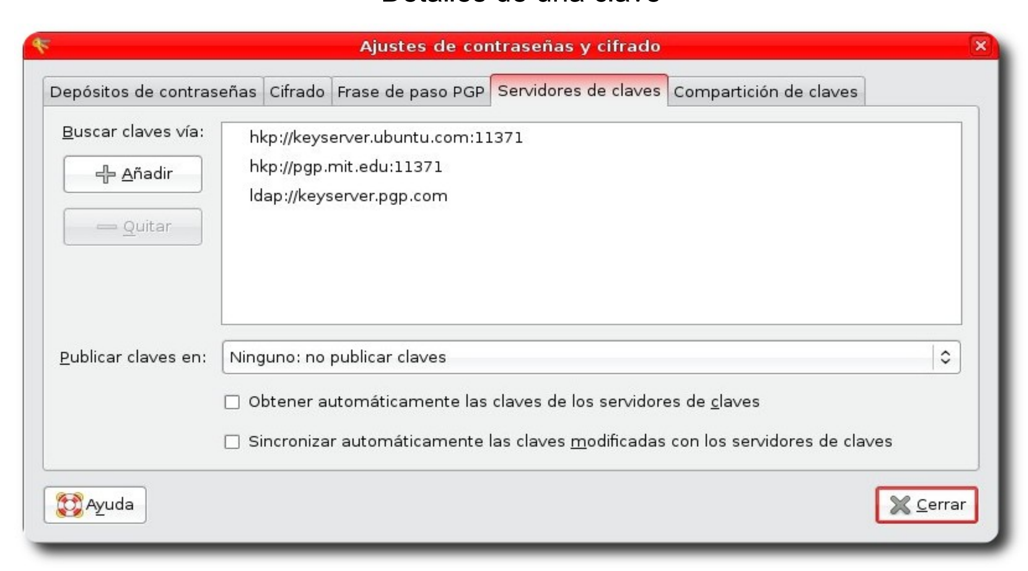
Creación de un par de claves



Niveles de confianza de una clave



Detalles de una clave



Configuración de servidores de claves públicos

Servidor de claves

Para muchos una de las mejores formas de poner a disposición nuestras claves públicas es mediante un servidor de claves. Servidores que están disponibles de forma pública por medio de Internet, estos servidores tienen distintas características, pero entre las más comunes se encuentran:

- ✔ Subir claves
- ✔ Bajar claves
- ✔ Publicar Claves
- ✔ Búsquedas de claves

Hoy por hoy contamos con una buena cantidad de servidores de claves públicas como ser:

- ✔ CryptNET Keyserver Network
  - ➢ gnv.keyserver.cryptnet.net
- ✔ pgp.net
  - ➢ wwwkeys.us.pgp.net
  - ➢ wwwkeys.nl.pgp.net
  - ➢ wwwkeys.ch.pgp.net
  - ➢ wwwkeys.uk.pgp.net
  - ➢ wwwkeys.cz.pgp.net
  - ➢ wwwkeys.de.pgp.net
  - ➢ wwwkeys.dk.pgp.net
  - ➢ wwwkeys.es.pgp.net
- ✔ www.keyserver.net Network
  - ➢ search.keyserver.net
  - ➢ seattle.keyserver.net
  - ➢ germany.keyserver.net
  - ➢ belgium.keyserver.net
  - ➢ finland.keyserver.net
  - ➢ thailand.keyserver.net
  - ➢ pgp.ai.mit.edu
  - ➢ pgp.cc.gatech.edu
  - ➢ pgp.es.net
  - ➢ pgp.rediris.es
  - ➢ pgp.uk.demon.net
  - ➢ pgp.uni-mainz.de
  - ➢ pgp.nic.ad.jp
  - ➢ ds.carnet.hr

pero también contamos con herramientas software que nos permiten implementar nuestro propio servidor de claves, que puede ser utilizado de forma local en nuestra empresa , organismo o universidad, o ponerlo a disposición de forma pública por medio de Internet.

Aplicaciones como:

- ✔ OpenPKSD
- ✔ SKS
- ✔ Onak
- ✔ Phkp-master

son las que nos permiten implementar nuestro propio servidor de claves; por temas demostrativos hemos implementado un servidor local de claves haciendo uso de la aplicación Onak, cuya pequeña demostración la tenemos en las siguientes imágenes.

Onak

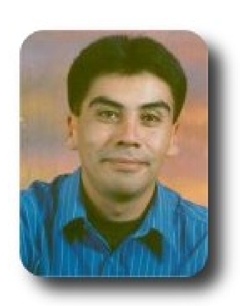
Onak es un servidor de claves compatible OpenPGP y soporta múltiples subclaves, fotos, ids y relación entre llaves.

Este provee una interfaz HKP compatible al momento de hacer uso el parámetro `–keyserver` de gnupg al momento de realizar importaciones, exportaciones y búsquedas de claves.

Referencias

[1] http://www.gnupg.org/

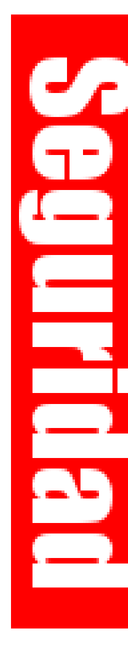
Autores



Esteban Saavedra López
Líder de la Comunidad ATIX (Oruro – Bolivia)
Activista de Software Libre en Bolivia
jesaavedra@opentelematics.org
http://jesaavedra.opentelematics.org



Joseph Sandoval Falomici
Profesor universitario
Entusiasta de Software Libre
josephsandoval@gmail.com



La Entrevista



Julian Carlo Fagotti

Coordinador Latinoware



1. Cuáles fueron las principales motivaciones para organizar Latinoware.

En 2003, cuando el gobernador requiria ganar las elecciones en Paraná, entonces determina el uso de software libre para la Administración Pública. Como esto no era suficiente para hacerlo, pusimos, en marcha la Primera Conferencia Internacional de Software Libre en 2003, en Curitiba. La Itaipú en el momento fue uno de los patrocinadores del evento.

En 2004, la Celepar propone a Itaipú, un evento centrado en la integración latinoamericana. Nació por lo tanto, el concepto de Latinoware. La Itaipú deja la organización para ser patrocinadora, y más que eso el Mayor socio! Las condiciones geográficas de Paraná son muy favorables , con una triple frontera entre Argentina y Paraguay, un puerto para el Atlántico desde varios países de América Latina, además de Itaipú, que es una empresa binacional (Brasil

1. Cuáles fueron las principales motivaciones para organizar Latinoware.

Em 2003, quando o Governador Requião ganhou as eleições no Paraná, determinou o uso de software livre para a administração Pública. Como não basta fazer, tem que compartilhar, lançamos a Primeira Conferência Internacional de Software Livre, em 2003, em Curitiba. A Itaipu era na época uma patrocinadora do evento.

Em 2004, a Celepar propõe à Itaipu um evento focado na integração latino americana. Nasce daí o conceito de Latinoware. A Itaipu deixa de ser patrocinadora para ser organizadora. Mais do que isso. Grande parceira! As condições favoráveis são a situação geográfica do Paraná, com uma tríplice fronteira entre Argentina e Paraguai, um porto para o Atlântico de vários países latino americanos, somada à Itaipu, que é uma empresa binacional (Brasil - Paraguai), a maior

- Paraguay), el mayor generador de energía hidroeléctrica del mundo. Es decir, Paraná y la Itaipú tienen una vocación hacia la integración latinoamericana, junto con la decisión política de los dirigentes de éstas empresas, y el apoyo de la comunidad de software libre sólo podría hacerse en Latinoware.

La idea de los eventos de software libre, con sus conferencias y talleres, es también un lugar para los desarrolladores y usuarios del mundo del software libre para conocerse personalmente (es muy común en esta red de personas que comparten sólo saber por e-mail) -- y ¿por qué no? -- Confraternizar directamente sus propios logros. Esto hace Latinoware y muchos eventos que tenemos en América Latina.

Independientemente de que ganó las elecciones, ya habíamos visto las transformaciones políticas en curso en América Latina: la consolidación de la democracia. En cuanto a resultados, existen personas a quienes les gusta y a quienes no esta historia, dentro del proceso democrático, lo que llevó al poder a **Lula, Chaves, Evo Morales, Lugo**, dar una perspectiva diferente para América Latina. Es una oportunidad única que ver un continente que tienen en el software libre: **el compartir el conocimiento para coadyuvar al desarrollo económico y social.**

Latinoware nace de los cambios políticos, que se criado en los cambios tecnológicos y culturales.

2. Qué instituciones u organismos, fueron los principales precursores para el nacimiento de Latinoware?

El movimiento del software libre de Paraná, la Celepar – Informática de Paraná, la Itaipú, el Parque Tecnológico de Itaipú - PTI. Pero debemos recordar que la Itaipú Celepar, y desde hace décadas, la novedad fue el cambio de dirigentes. El PTI es la creación de

geradora de energia hidroelétrica do mundo. Ou seja, o Paraná e a Itaipu que têm uma vocação para a integração latino americana, junto com a decisão política dos dirigentes destas empresas, e apoio da comunidade de software livre só podia dar na Latinoware.

A idéia dos eventos de software livre, com suas palestras e oficinas, é também ter um lugar para desenvolvedores e usuários do mundo do software livre se conheçam pessoalmente (é muito comum nesta rede de compartilhamento as pessoas só se conhecerem por e-mail) – e porque não? – confraternizar-se pelos seus feitos. Isso é a Latinoware e os inúmeros eventos que temos na América Latina.

Independente de quem ganhasse as eleições, já tínhamos víamos as transformações políticas da América Latina em andamento: a consolidação da democracia. Quanto aos resultados, há quem goste, há quem não goste, mas esta história, dentro do processo democrático, que levou ao poder Lula, Requião, Chaves, Evo Morales, Lugo, dão uma perspectiva diferente para a América Latina. É uma oportunidade única de fazermos com o Continente o que se faz com o software livre: dividir conhecimento para somar desenvolvimento econômico e social.

A Latinoware nasce das mudanças políticas, para ser criado para as mudanças tecnológicas e culturais.

2. Que instituciones u organismos, fueron los principales precursores para el nacimiento de Latinoware?

O Movimento Software Livre Paraná, a Celepar – informática do Paraná, a Itaipu, o Parque Tecnológico de Itaipu – PTI. Mas devemos lembrar que a Celepar e a Itaipu existem há décadas, a novidade foi a mudança dos dirigentes. O PTI é criação desta atual gestão da Itaipu.

esta actual gestión de la Itaipú.

Por lo tanto, tenemos que citar a los dirigentes que deciden que hacer. En el primer Latinoware, Marcos Mazoni es el presidente de Celepar, hoy es el presidente de la compañía SERPRO del gobierno federal, que también está en Latinoware, y el doctor Nizan es presidente de Celepar, que da continuidad la política de gobierno y, por consiguiente, el apoyo la Latinoware. George Samek es presidente de la Itaipú, Marli Portella es superintendente de Informática. Nelson de Marco es presidente del PTI. Antes fue el Juan Sotuyo. Este es un buen ejemplo de continuidad de la política de software libre. Esta es la quinta edición del evento. Esta es una historia de América Latina, el evento es un momento de celebración de victorias, y el examen de lo que no estamos satisfechos. De esta contabilidad, el Gobierno de Paraná y el Gobierno Federal, el saldo es sumamente positivo. Este caso de éxito, también queremos compartir con más de 20 conferencistas.

3. Los objetivos de Latinoware, se están logrando como se espera?, o existe algún obstáculo principal?

El evento esta en alza. Cada año, resulta mejor que el anterior. Tanto la calidad de conferencias, talleres, como el número de participantes y el número de países participantes.

El principal obstáculo es la cultura. Brasil ha estado siempre a la espalda a sus vecinos. Los generales de los períodos dictatoriales hablaban entre si, pero no las personas. Hoy en día hay avances, sobre todo en la integración económica.

Encontrar las experiencias de software libre en la región, facilitar la llegada de público de América Latina en un continente de este tamaño no es fácil. Con los conferencistas para dar un ejemplo. El problema es que traer

Por isso temos que citar os dirigentes que decidem fazer. Na primeira Latinoware, Marcos Mazoni era presidente da Celepar, hoje é presidente do SERPRO empresa do governo federal, que também está na Latinoware, e o Dr. Nizan é o presidente da Celepar, que deu continuidade à política de governo e, conseqüentemente, o apoio à Latinoware. O Jorge Samek é o presidente da Itaipu, a Marli Portella é superintendente de Informática. O Nelson de Marco é presidente do PTI. Antes foi o Juan Sotuyo. Isso um bom exemplo de continuidade da política de software livre. Estamos na quinta edição do evento. Esta é uma história latino americana, o evento é um momento de celebração das vitórias e, revisão do que não deu certo. Nesta contabilidade, no Governo do Paraná e do Governo Federal, o saldo é extremamente positivo. É esse caso de sucesso, também queremos compartilhar com mais de 20 palestrantes.

3. Los objetivos de Latinoware, se están logrando como se espera?, o existe algún obstáculo principal?

O evento é ascendente. Cada ano, melhor que último. Tanto na qualidade das palestras, das oficinas, quanto no número de participantes, o número de países que participam.

O grande obstáculo é cultural. O Brasil sempre foi esteve de costas para seus vizinhos. Os generais dos períodos ditatoriais falavam entre si, mas o povo não. Hoje há avanços, principalmente na integração econômica.

Localizar as experiências de software livre da região, viabilizar a vinda de público latino americano num continente deste tamanho não é fácil. Com os palestrantes até damos um jeito. O problema é trazer público que está há 2, 3, 4 mil quilômetros.

público que esta a 2, 3, 4 mil kilómetros.

No tenemos líneas áreas frecuentes de toda America latina a Foz de Iguazu. Se trata de un problema de la logística del continente. Si pudiera interferir en una sola cosa para cualquier iniciativa de integración, escogería los vuelos a precios más populares. Es esencial para la integración en un continente de este tamaño.

El hecho de responder a esta entrevista en portugués, se muestra otro pequeño problema. Hablamos dos idiomas. Pero estos no son insuperables “la Unión Europea la ha realizado" Hablando en Europa, hay que tener cuidado, porque el modelo de integración tiene un fuerte sesgo imperialista, de mantener a los países pobres sin el desarrollo de tecnología. Qué es la intensión inversa de Latinoware.

4. Cuál consideras, el mejor y peor acierto que haya tenido Latinoware desde su inicio.

El mayor éxito fue hacer un evento de tecnología, de software libre, dentro del programa de integración de América Latina. Otra cosa fue definir un lugar del evento, y tener como socio, el Tecnológico de Itaipú, con una fantástica infraestructura, que es mejor cada año.

El error más grande fue la primera en 2004, subestimar la logística de transporte de América Latina. El Internet está llegando a muchas personas pero no el Internet trae la gente. Subestimamos también la dificultad de comprender la ventaja competitiva de la cooperación en las empresas. Que no acaban siendo errores, pero tenemos dificultades, y vamos a superarlas poco a poco. Por supuesto, hubo muchos errores, pero no hay nada que no se pueda corregir. Pero estas dificultades escapan de la organización del evento, pero las trataremos más adelante.

Ah ... siempre tiene criterios distintos, la llegada de Stallmann, hay gente que piensa

Não temos linhas aéreas freqüentes de todo lugar da América Latina até Foz do Iguaçu. Este é um problema de logística do continente. Se eu pudesse interferir numa única coisa para qualquer iniciativa de integração, escolheria a aviação à preços populares. É fundamental para toda e qualquer integração num continente deste tamanho.

O fato de eu estar respondendo esta entrevista em português, mostra um outro pequeno problema. Falamos dois idiomas. Mas se isso não fosse superável, “the unificazione européia nicht effectuer”. Falando em Europa, temos que ficar atentos, porque o modelo de integração deles tem um forte viés imperialista, mantendo os países pobres sem desenvolvimento próprio de tecnologia. Que é a intenção inversa da Latinoware.

4. Cuál consideras, el mejor y peor acierto que haya tenido Latinoware desde su inicio.

O maior acerto foi fazer um evento de tecnologia, de software livre, dentro da agenda da integração latino americana. Outra coisa foi ter definir como local do evento, e ter como parceiro, o Tecnológico de Itaipu, com uma infra-estrutura fantástica, que está a cada ano melhor.

O maior erro foi na primeira, em 2004, subestimar a logística de transporte latino americana. A internet está chegando para muitas pessoas, mas a internet não traz as pessoas. Subestimamos também a dificuldade do entendimento da vantagem competitiva da cooperação nas corporações. Que acabam não sendo erros, mas dificuldades que temos, e vamos aos pouco superando. Claro que houve erros, inúmeros, mas nada que não esteja sendo corrigido. Mas estas duas dificuldades fogem à organização do evento, ainda que tratemos do assunto.

que fue el mayor éxito, y hay gente que cree que fue un error. Mad Dog por unanimidad fue positivo. Ambos son de la Free Software Foundation.

5. Qué relación mantiene Latinoware con instituciones u organismos estatales y/o privados?

Latinoware tuvo el apoyo inicial de la voluntad política de Itaipú y la Celepar, que son sus organizadores. Otras empresas e instituciones también han patrocinado el evento, el envío de otros oradores participantes.

La relación desde el punto de vista de patrocinio, estamos muy flexibles, tenemos una propuesta de patrocinio por defecto, pero aceptamos contrapropuestas. Si alguien quiere patrocinar, pero en lugar de dar dinero a Brasil, quiere mandar un avión lleno de bolivianos de las comunidades de software libre, para que participen en las conferencias y talleres, estamos de acuerdo.

6. Qué organismos o instituciones financian la realización de Latinoware?

Tanto empresas privadas como estatales son patrocinadoras, pero con un predominio de Estado y de Gobierno. El mercado ha tomado esta gran corriente de trabajo que es la comunidad de software libre, pero no todos los eventos los retribuyen, o incluso a las mismas comunidades.

Para las empresas privadas tenemos un cuento simple, especialmente para los fabricantes de hardware. Cuanto más ahorros en América Latina en licencias y royalty, sin ser piratería, puede comprar más hardware. El programa de ordenador para Todos de Brasil y Paraná Digital son buenos ejemplos. Para los productores de software, la capacidad de producción de América Latina es enorme, basta con una conexión y hardware. Además de ser un continente con

Ah... tem sempre o folclore sobre a vinda do Stallmann. Gente que acha que foi o maior acerto, e gente que acha que foi erro. Já o Mad Dog é uma unanimidade positiva. Ambos são da Free Software Foundation.

5. Que relación mantiene Latinoware con instituciones u organismos estatales y/o privados?

A Latinoware teve como apoio inicial a vontade política da Itaipu e da Celepar, que são seus organizadores. Outras empresas e instituições tem patrocinado o evento, outros participam mandando palestrantes.

A relação do ponto de vista de patrocínio, somos bastante flexível, temos uma proposta de patrocínio padrão, mas aceitamos contrapropostas. Se alguém quer patrocinar, mas ao invés de dar dinheiro para o Brasil, quiser mandar um avião cheio de Bolivianos das comunidades de software live, ou interessados em software livre, que efetivamente participe das palestras e oficinas, a gente aceita.

6. Que organismos o instituciones financian la realización de Latinoware?

Tanto empresas estatais como privadas são patrocinadoras, mas ainda com uma predominância de estatais e governos. O mercado tem se aproveitado deste grande work-flow que é a comunidade Software livre, mas nem todos retribuem aos eventos, ou mesmo diretamente às comunidades.

Para as empresas privadas temos uma conta simples, especialmente para os fabricantes de hardware. Quanto mais a América Latina economizar em licenças e royaltes, sem ser pirataria, mais hardware poderá comprar. O programa computador Para Todos do Brasil e o Paraná Digital são bons exemplos. Para produtores de software, a capacidade de

una capacidad de consumo creciente, ávidos de tecnología. Si no tenemos más patrocinares privados, el error es de ellos. Pero ellos son rápidos y no les gusta cometer errores.

7. Cuál el papel principal que tienes dentro de Celepar y Latinoware?

Mi cargo es asesor para asuntos institucionales y las relaciones con la comunidad, hacer que la relación entre la empresa y las comunidades de software libre y otras instituciones. Así que, naturalmente, mi actividad en eventos, y en la coordinación de la Latinoware, es la misma que en Celepar. Yo soy uno de los coordinadores del Movimiento Software Libre Paraná.

En Latinoware soy uno de los coordinadores, junto con Siriaco de Itaipú Malinverni el PTI, (quiero hacer una mención a Jaime Nascimento, que estuvo en la coordinación desde el principio).

Tengo mucha actividad política. Hay cierta dificultad para algunas personas de la comunidad que no aceptan que no programe. Pero eso está cambiando. Porque quien contrata programadores y usa programas informáticos, no necesariamente programa.

Esto ocurre siempre a un grupo que está creciendo mucho. Los pioneros sienten la necesidad de diferenciar, lo que creen justo. Después de todo, no sé como comencé con el software libre. Lo que no se puede dejar es que el movimiento crezca. Estoy loco para ver el día en que los "patriotas" entren en la comunidad del software libre y se pongan a discutir con los "nerds". Después de todo quiere todo el mundo utilizar el software libre, ¿no?

8. Qué impacto consideras que tiene el organizar eventos como Latinoware?

Desde el punto de vista tecnológico es

produção latino americana é enorme, basta dar conexão e um hardware. Além de sermos um continente com capacidade de consumo cada vez maior, ávidos por tecnologia. Se não temos mais patrocinares privados o erro é deles. Mas eles são rápidos e não gostam de errar.

7. Cual el papel principal que tienes dentro de Celepar y Latinoware?

Meu cargo é de assessor para assuntos institucionais e relações com a comunidade, faço a relação entre a empresa e as comunidades de software livre e outras instituições. Sendo assim é natural minha atividade em eventos, e na coordenação da Latinoware, a qual a Celepar foi a proponente inicial. Sou um dos coordenadores do Movimento Software Livre Paraná.

Na Latinoware sou um dos coordenadores, junto com o Siriaco da Itaipu e o Malinverni do PTI, (quero aqui fazer uma menção ao Jaime Nascimento, que esteve na coordenação desde a primeira).

Faço muita atividade política. Existe uma certa dificuldade de algumas pessoas da comunidade aceitarem quem não programa. Mas isso vem mudando. Até porque quem contrata programação, e usa os programas e sistemas, também não programa necessariamente.

Isto sempre acontece com um grupo que está crescendo muito. Os pioneiros sentem a necessidade de se diferenciarem, o que eu acho justo. Afinal, foram eles e não eu quem comecei com o software livre. O que não pode é não deixar o movimento crescer. Estou louco para o ver o dia em que as “patricinhas” entrarem na comunidade de software livre e discutirem com os “nerds”. Afinal queremos que todo mundo use software livre, não?

8. Qué impacto consideras que tiene el organizar

emocionante, que rescata en este mundo la idea del mundo libre, donde el flujo de información no se basa en las ideas de patentes. Este mundo de las patentes intenta ser confundido con el desarrollo capitalista en los dos últimos siglos, pero en realidad, hoy es un obstáculo al libre comercio. Para América Latina la lógica del patente de mercado es cruel. No hemos podido patentar nuestras ideas, que no sea local o internacionalmente. Y para empeorar, la industria de patentes deja que copulate (tipo de chocolate copuaçu típico de la Amazonía) fue registrado por una empresa japonesa. Tomó años para que la Organización Mundial del Comercio reconozca que era una patente bizarra.

Un evento trata de cosas importantes para América Latina. La idea de desarrollo económico basado en el intercambio, es como un guante para América Latina. Y funciona tan bien dentro del capitalismo que los Estados Unidos que sigue siendo uno de los mayores desarrolladores de código abierto. Esperamos tener un impacto en la economía de los países participantes. Sólo la provincia de **Paraná economiza más de 150 millones de reales por licencias y royalty**. Este dinero es importante para mejorar el sueldo de los maestros, para el ámbito de la salud.

9. Cómo consideras que la comunidad de Software Libre en América Latina podría colaborar o tener mayor participación en Latinoware?

La gente precisa hablar más, Latinoware es para eso. Queremos crear una comunidad de software libre que está conectado con el mundo, sino para resolver los problemas de su propio país. Hacer la encuesta de su propio país, provincia o ciudad de sus necesidades, que se aplica a las empresas ayuda a traer oportunidades para el desarrollo de los sistemas y migrarlos a software libre. Traer los problemas comunes

eventos como Latinoware?

Do ponto de vista tecnológico é empolgante, quem entra neste mundo resgata a idéia de mundo livre, onde os fluxos de informações não são baseados em patenteamento de idéias. Este mundo de patenteamento tenta se confundir com o desenvolvimento capitalista dos últimos dois séculos, mas na verdade, hoje é um empecilho de livre comércio. Para a América Latina a lógica do mercado patenteado é cruel. Não conseguimos patentear nossas idéias, nem local nem internacionalmente. E para piorar, a indústria do patenteamento deixou que o copulate (espécie de chocolate de copuaçu típico da amazônia) fosse registrado por uma empresa japonesa. Demorou anos para a Organização Mundial do Comércio reconhecer que era um patente bizarra.

O evento trata de coisas importantes para a América Latina. A idéia de desenvolvimento econômico baseado no compartilhamento, cabe como uma luva para a América Latina. E funciona tão bem dentro do capitalismo que os Estados Unidos é ainda um dos maiores desenvolvedores de código aberto. Esperamos ter um impacto na economia dos países participantes. Só a província do Paraná economizou mais de 150 milhões de reais com licenças e royaltes. Este dinheiro foi importante para a melhor remuneração dos professores, para a área de saúde.

9. Cómo consideras que la comunidad de Software Libre en América Latina podría colaborar o tener mayor participación en Latinoware?

A gente precisa se conversar mais, a Latinoware é para isso. Queremos criar uma comunidade de software livre que esteja conectada com o mundo, mas que resolva os problemas de seu próprio país. Fazer o levantamento do que seu próprio país, província, ou cidade precisa, o que vale para

y tratare de resolverlos juntos. Estamos formando una comunidad Latinoware para que podamos desarrollar las soluciones para el mundo que nos interesa. De este modo, incluso los que no pueden ir a Foz de Iguazu a finales de septiembre, podrían ayudar. Queremos que Latinoware sea la base de una importante corriente de trabajo en América Latina.

10. Qué recomendarías a los gobiernos y universidades en América Latina con respecto a organizar eventos como Latinoware?

El evento no es el más importante. Lo importante es la opción alternativa de software libre. De otro modo, hacer un gran evento, regresar a casa, abrir sus ventanas y siguen utilizando los productos pirateados ser sancionados por la Organización Mundial del Comercio, o prisionero de renovar licencias, enviando dinero a aquellos que ya tienen. Hacer un evento que forma parte de la opción por el software libre, tienen el compromiso de iniciar el cambio de cultura dentro de las propias instituciones. Tiene gente y dinero para hacer esto. Recordemos que el "libre" es libertad y no gratis. La diferencia está en hacer que los líderes locales, utilicen el dinero en su propio país, pero con el apoyo de una comunidad internacional.

11. Cuáles los planes y actividades a futuro que tiene previsto Latinoware?

No queremos que Latinoware sea solo un evento, sino que sea una fecha de referencia para compartir soluciones en América Latina con el resto del mundo. Estamos dispuestos a hacer eventos en cualquier país de América Latina. Pero tenemos que reunirnos una vez al año con todo el mundo. Podemos hacer Latinoware Amazonas, Latinoware de Centroamérica. Todo para centrar soluciones más adecuadas a las regiones. Pero tenemos que coordinar las fechas. La lógica es

empresas ajuda a trazer as oportunidades de desenvolvimento dos sistemas e migrações para software livre. Trazer os problemas comuns pra ser solucionado juntos. Estamos formando a comunidade Latinoware, para que possamos desenvolver com o mundo as soluções que nos interessam. Assim, mesmo quem não pode ir à Foz do Iguaçu no fim de setembro, poderá contribuir. Queremos que a Latinoware seja base de um grande work-flow latino americano.

10. Qué recomendarías a los gobiernos y universidades en América Latina con respecto a organizar eventos como Latinoware?

Evento não é o mais importante. O importante é a opção pela alternativa do software livre. Senão você faz um evento ótimo, volta para casa, abre seu windows e continua usando produto pirata e sendo punido Organização Mundial do Comércio, ou prisioneiro de renovação de licenças, mandando dinheiro para quem já tem. Fazer um evento faz parte da opção pelo software livre, ter o compromisso de inciar a mudança de cultura dentro das próprias instituições. Ter gente e verba para fazer isso. Vamos lembrar que o “free” é de livre e não de grátis. A diferença é fazer com as cabeças locais, que usam o dinheiro no seu próprio país, mas com o apoio de uma comunidade internacional.

11. Cuáles los planes y actividades a futuro que tiene previsto Latinoware?

Não queremos que a Latinoware seja só um evento, mas que ele seja uma data de referência no compartilhamento das soluções da América Latina com o resto do mundo. Estamos dispostos a fazer eventos em qualquer país da América Latina. Mas a gente tem que se reunir uma vez por ano com todos. Podemos fazer Latinoware Amazônica, Latinoware da América Central.

compartir y no competir. Además de crear una comunidad de desarrollo para resolver nuestros problemas como cito más arriba. A pesar de México y Brasil son los países más ricos, tenemos también pobreza y la falta de recursos para todos los sistemas que precisamos desarrollar para aumentar nuestra capacidad de producción. Entonces, es un problema para nosotros y para otros. ¿Por qué no compartir las soluciones? Luego hacer ajustes en las adaptaciones al portugués para compartir con Portugal y Angola, o a la inversa, en español para compartir con España ... También pensamos en gente que va a traducir en Inglés y Mandarín, debemos hacer que la gente comience.

12. Un mensaje para la comunidad de Software Libre en Bolivia.

El software es bueno para los gobiernos, para la economía, para el ocio, y la libertad es mejor todavía. Que su comunidad sea nuestra comunidad. Bolivia está sufriendo importantes transformaciones, y el software libre debe estar alerta. Me gustaría que la comunidad del software libre en Bolivia, además de venir a Foz, sea nuestra puerta para invitar a cualquier persona que usted cree necesario ir a Latinoware, que son los líderes de negocios y el gobierno. Queremos aportar soluciones que pueden aplicarse en Bolivia para los bolivianos. Vengan a Latinoware!

Tudo para focar soluções mais adequadas às regiões. Mas precisamos de coordenação das datas. A lógica é compartilhar e não concorrer. Além de criamos uma comunidade de desenvolvimento para resolvermos nossos problemas como eu cite acima. Apesar do Brasil e México serem os países mais ricos, temos também pobreza, e sempre falta recurso para todos os sistemas que precisamos desenvolver para aumentar nossa capacidade de produção. Então, o que é problema para um de nós, é problema para outro. Porque não compartilhar as soluções? Depois a gente faz as interfaces e adaptações em português para compartilhar com Portugal e Angola, ou o inverso, em espanhol para compartilhar com a Espanha... Tá bom, a gente vai pensar em traduzir para o inglês e o Mandarim também, mas deixa a gente começar.

12. Un mensaje para la comunidad de Software Libre en Bolivia.

Software é bom para governos, para a economia, para o lazer, e com liberdade é melhor ainda. Que sua comunidade seja a nossa comunidade. A Bolívia está passando por transformações importantes, e o software livre deve estar em pauta. Gostaria que a comunidade de software livre da Bolívia, além de vir para Foz, fosse nossos porta vozes para convidar quem vocês acham importante ir para a Latinoware, que são os dirigentes de empresa e governo. A gente quer apresentar soluções que possam ser implementadas na Bolívia pelos bolivianos. Venham para a Latinoware!




ATIX
Noticias

Festival de Instalación de BoliviaOS





Estuche de BoliviaOS y Tux



Miembros de la Comunidad preparando detalles



Guiando a los asistentes



Alegría durante el evento



Terminado el festival, siempre cae bien un buen refrigerio

Eventos y BoliviaOS



El **XV Congreso Nacional de Ciencias de la Computación CCBOL 2008**, será otro escenario donde el Software Libre sentará presencia, formando parte de algunas de las conferencias y de las mesas redondas a realizarse dentro de la agenda programada para este evento.

Un aspecto que cobra expectativa sera la mesa redonda donde delegados de la Comunidad de Software Libre de Bolivia, debatirán el tema de la presencia del Software Libre dentro la Universidad, la enseñanza superior y su contribución a aspectos académicos – investigativos.





Adicionalmente la comunidad de Software Libre Bolivia, estará presente en este evento para seguir promocionando la distribución BoliviaOS, como una mas de las estaciones dentro la gira promocional que se tiene programada en algunas instituciones y universidades de Bolivia.

Esta gira se realiza en coordinación entre la comunidad de Software Libre a nivel nacional y las comunidades de Software Libre locales

www.boliviaos.org



CONASOL 2008

8vo Congreso Nacional de Software Libre

La Paz - Bolivia

noviembre 2008

Comics


SEÑOR... DESCUBRIERON EL CÓDIGO DEL GENOMA HUMANO
¡¡MALDITOS HACKERS!! VOY A TENER QUE CAMBIAR LA CONTRASEÑA
Daniel PAZ



Conociendo lo Nuestro

Beni

Turismo y Libertad



Trinidad, capital del departamento de Beni



Llanos de Beni



Vista panorámica de la Amazonia del Beni

Vista panorámica de Trinidad - Beni



Flotel – Amazonas - Beni



Festividad de San Ignacio - Beni

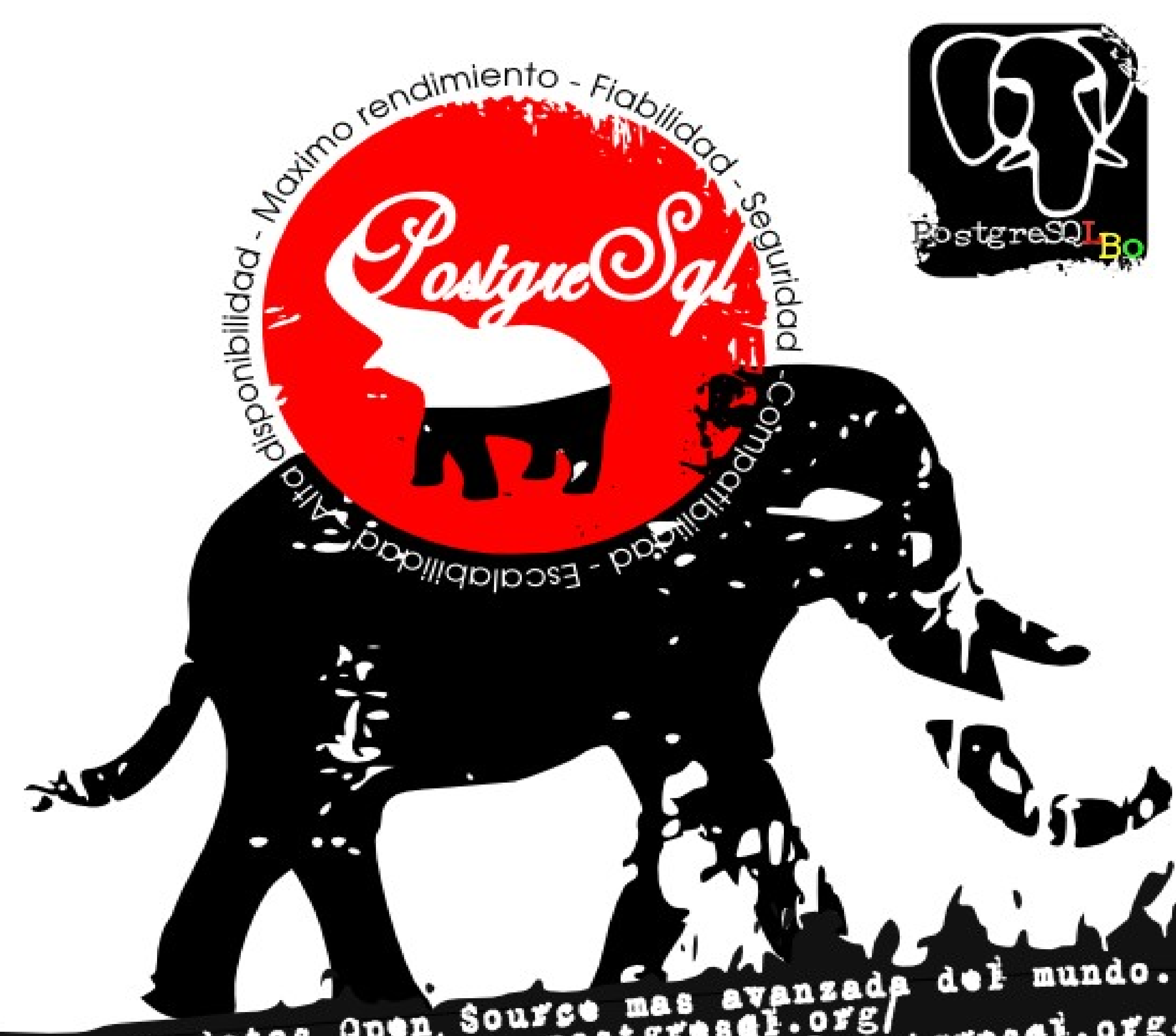
Libres para pensar, libres para decidir, libres para crear



Te ofrecemos este espacio para mostrar tu Creatividad

Envíanos tus diseños y creaciones para publicarlos

En una manada siempre hay un Líder



La base de datos Open Source mas avanzada del mundo.
Sitio:http://www.postgresql.org/
Lista:pgsql-es-ayuda@postgresql.org.

Jared Lopez

Consultas

Contacto

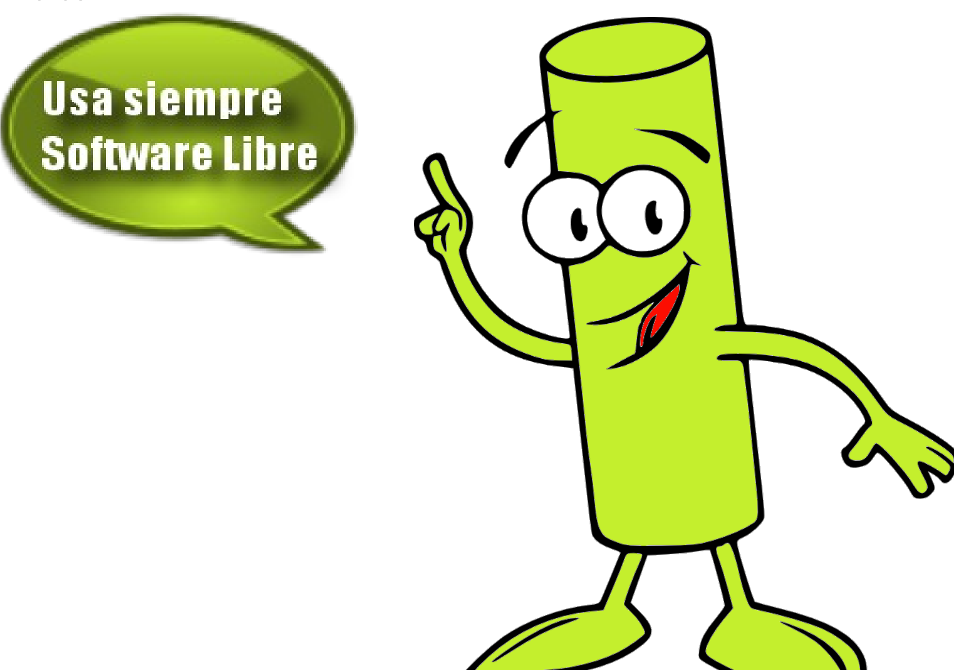
Para solicitar cualquier información, puedes contactar a:

- Esteban Saavedra López (jesaavedra@opentelematics.org)
- Williams Chorolque Choque (williamsis@gmail.com)

Publicación

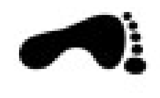
Te invitamos a ser parte de la **Revista ATIX**. La forma de participar puede ser enviándonos:

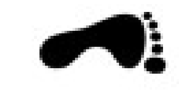
- Artículos referidos a áreas como:
  - Instalación y personalización de Aplicaciones
  - Scripting
  - Diseño gráfico
  - Programación y desarrollo de aplicaciones
  - Administración de servidores
  - Seguridad
  - y cualquier tema enmarcado dentro del uso de Software Libre
- Trucos y recetas.
- Noticias.
- Comics.
- Links de interés.

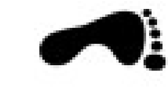
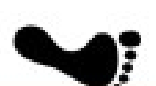




Marcamos Huella





http://atix.opentelematics.org